

MultiCash® 3.23

Kommunikation

Benutzerhandbuch

Omikron Systemhaus GmbH & Co. KG
Von-Hünefeld-Str. 55
D-50829 Köln

Tel.: +49 (0)221 -59 56 99 -0
Fax: +49 (0)221 -59 56 99 -7

info@omikron.de
www.omikron.de

Einleitung

Dieses Dokument wurde für die elektronische Verteilung und den bedarfsgerechten Ausdruck auf einem Laserdrucker konzipiert. Daher wurden Schriften und Layout für ein optimales Druckergebnis gewählt; die Bildschirmanzeige stand erst an zweiter Stelle.
Dem gezielten Aufsuchen bestimmter Informationen dienen das Gesamt-Inhaltsverzeichnis am Anfang des Dokuments sowie die Zwischen-Inhaltsverzeichnisse zu Beginn eines jeden Kapitels. Durch Anklicken eines bestimmten Verzeichniseintrages (Mauszeiger ändert sich in ☝) gelangen Sie auf die entsprechende Seite im Handbuch.

Drucken dieses Handbuches

Das vorliegende PDF-Dokument wurde zum Drucken auf Papier im DIN A4-Format optimiert. Drucken Sie bei Bedarf das Handbuch oder Teile davon über die Druckfunktion Ihres Acrobat-Readers aus.

Informationen zur Verwendung dieses Handbuches

Weitere Informationen zur Verwendung des Handbuches finden sie in Kapitel 3.1 des Basismodul-Handbuches.

Online-Hilfe

Für Hypertext-Navigation am Bildschirm steht Ihnen die Online-Version des Handbuches zur Verfügung, die Sie aus dem Programm aufrufen. Informationen zum Aufruf finden Sie in Kapitel 3.2 des Basismodul-Handbuches. In der Online-Hilfe haben Sie neben der Navigation über das Inhaltsverzeichnis (Registerkarte Inhalt) auch die Möglichkeit zur Schlüsselwortsuche (Registerkarte Index) bzw. zur Volltextsuche (Registerkarte Suchen).

Copyright

Alle Angaben in diesem Handbuch wurden mit größter Sorgfalt erarbeitet und getestet. Trotzdem sind Fehler nicht ganz auszuschließen. Omikron kann weder eine juristische Verantwortung, noch irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen. Für Verbesserungsvorschläge, Hinweise auf Fehler und jedwede qualifizierte Kritik sind wir dankbar.

Omikron Systemhaus



Inhaltsverzeichnis


MCC



Inhaltsverzeichnis: Kapitel 1

Seite



1 Datenfernübertragung

Das Programmsystem stellt verschiedene Kommunikationsprozesse zur Datenfernübertragung zur Verfügung.

Zusammen mit dem Basismodul wird immer das Kommunikationsverfahren ZVDFÜ installiert. Die Installation anderer Kommunikationsverfahren (wie FTAM, FTP, EBICS, HBCI/HBCI+, ETEBAC) ist optional möglich.

Eine Sonderform des Kommunikationsverfahren ZVDFÜ ist MCFT, die neben dem Vorteil einer gesicherten Übertragung von komprimierten Daten auch die Abbildung unternehmensinterner Unterschriftshierarchien durch die Elektronische Unterschrift ermöglicht. Die Unterschriftsprüfung erfolgt hier "online", so dass der Kunde sofort über die Gültigkeit der versandten Unterschriften informiert wird. Auch das Kommunikationsverfahren MCFT wird standardmäßig installiert.

Zur Nutzung von MCFT muss - genauso wie bei Anwendung des Kommunikationsverfahrens FTAM - das Zusatzmodul "Elektronische Unterschrift" installiert werden.

Die notwendigen Einstellungen zur Datenfernübertragung mit den verschiedenen Kommunikationsverfahren nehmen Sie über das Menü Kommunikation vor.

Näheres zur Bedeutung der prozessspezifischen DFÜ-Antwort-Codes erfahren Sie in Kapitel 5.4:

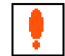
ZVDFÜ-Antwort-Codes
MCFT-Antwort-Codes
FTAM-Antwort-Codes
FTP-Antwort-Codes
EBICS-Antwort-Codes

Die Bedeutung spezieller Verschlüsselungs-Antwort-Codes bei FTAM- bzw. FTP-Übertragungen wird in Kapitel 4.5.2: *DFÜ-Returncodes im Rahmen der Verschlüsselung* erläutert.



1.1 Kommunikation

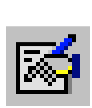
Im Menü -Kommunikation- werden u. a. DFÜ-Parameter gesetzt, Bankparameterdateien (BPD) erstellt bzw. geändert, Dateien im Dateimanager unterschrieben und versandt etc.



Die Untermenüpunkte -Tanliste pflegen- und -Zeiträume pflegen- werden nur dann angezeigt, wenn Sie die Zusatzmodule "HBCI" bzw. "HBCI^{+}" installiert haben.
Der Untermenüpunkt -Verschlüsselung- wird nur angezeigt, wenn Sie die Zusatzmodule "FTAM" bzw. "FTP" installiert haben.

Näheres zu den Menüpunkten finden Sie in Kapitel 2: *Menü Kommunikation*.

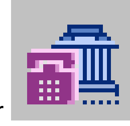
Darüber hinaus werden in der Symbolleiste folgende Symbole angezeigt, die Kommunikationsfunktionen betreffen:

 oder 

Dieses Symbol entspricht dem Menüpunkt -Kommunikation- / -Datei-Manager-.

 oder 

Dieses Symbol entspricht dem Menüpunkt -Kommunikation- / -DFÜ-Favorit ausführen -.

 oder 

Dieses Symbol entspricht dem Menüpunkt -Kommunikation- / -Assistent Abholen von Daten bei mehreren Banken -.



1.2 DFÜ-Verfahren

Das Programmsystem stellt verschiedene Kommunikationsprozesse zur Datenfernübertragung zur Verfügung.

Standardmäßig werden immer die Kommunikationsverfahren ZVDFÜ und MCFT installiert. Die Installation anderer Kommunikationsverfahren (FTAM, FTP, EBICS, HBCI/HBCI^{+}) ist optional möglich.

MCFT ist eine Sonderform des Kommunikationsverfahrens ZVDFÜ, das neben den Vorteilen der gesicherten Übertragung von komprimierten Daten auch die Abbildung unternehmensinterner Unterschriftshierarchien durch die Elektronische Unterschrift ermöglicht. Die Unterschriftsprüfung erfolgt hier "online", sodass der Kunde sofort über die Gültigkeit der versandten Unterschriften informiert wird.

Die Merkmale, die laut ZKA-Anforderungen Kennzeichen für ein optimales Kommunikationsverfahren sind, können den nachfolgenden (nach Electronic Banking und HomeBanking getrennten) Tabellen entnommen werden.

Electronic Banking:

	MCFT	**FTAM**	**FTP**	**EBICS**
Merkmal	spezielles, auf die Electronic Banking-Anforderungen zugeschnittenes Verfahren	Kombination von Standardverfah-ren	Kombination von Standardverfah-ren	Internet
Prüfung auf fehlerfreie Datenübertragung	ja	nur mit EU	ja	ja
Komprimierung	Ja (ZIP-Verfahren)	FLAM (wahlweise)	FLAM (wahlweise)	Ja (ZIP-Verfahren)
Verschlüsselung	Triple-DES mit asymmetrischem Schlüsselaus-tausch nach Diffie/Hellman	DES / RSA-Hybrid-Verfahren (wahlweise)	DES / RSA-Hybrid-Verfahren	TLS(SSL) und DES / RSA-Hybrid-Verfahren
Formatvalidierung	während der Übertragung	nach der Übertragung	nach der Übertragung	nach der Übertragung
Vorab-Autorisierungsprüfung	immer	nein	optional	optional
Mitteilung der Prüfungsergebnisse	sofort am Ende der Übertragung	später im Protokoll	sofort bzw. später	später im Protokoll
Autorisierung/ Manipulationsschutz	RSA-Unterschrift 1024 Bit RipeMD-160 direkte Prüfung (online)	RSA-Unterschrift 1024 Bit RipeMD-160 getrennte Dateien Prüfung offline	RSA-Unterschrift 1024 Bit RipeMD-160 optional: Vorab-Prüfung (online) ausführliche Prüfung: offline	RSA-Unterschrift 1024 Bit / 1536 - 4096 Bit RipeMD-160 / SHA-256 optional: Vorab-Prüfung (online) ausführliche Prüfung: offline
EU	ja (wahlweise)	ja (wahlweise)	ja (wahlweise)	ja
Verteilte EU	ja	nein	ja	ja



Kommunikationsmedien	Modem X.25 ISDN TCP / IP (Internet)	X.25 ISDN	TCP / IP (Internet)	TCP / IP (Internet)
Einsatzbereich	Electronic Banking Europa	Electronic Banking Deutschland	Electronic Banking deutsche Privatbanken	Electronic Banking Deutschland

HomeBanking:

	HBCI	HBCI+
Merkmal	Internet	Internet
Prüfung auf fehlerfreie Datenübertragung	TCP / IP	TCP / IP
Komprimierung	ja	ja
Verschlüsselung	ja	ja
Validierung (syntaktische Prüfung)	nein	nein
Autorisierung / Manipulations-schutz	RipeMD / RSA	PIN / TAN
EU	ja	nein
Verteilte EU	nein	nein
Kommunikations-medien	TCP / IP (Internet)	TCP / IP (Internet)
Einsatzbereiche	HomeBanking	HomeBanking

Die Kommunikationsverfahren bedienen sich unterschiedlicher Netze zur Datenübertragung, die nachfolgend noch einmal explizit aufgeführt sind.

Verfahren	Merkmal	Geschwindigkeit	Hardware	Sonstiges
X.25	Paketübermittlung öffentliche und private Netze	9.600 - 28.800 Baud abhängig vom PAD	Modem oder X.25-Karte	Service-Provider
ISDN	Digitale Übermittlung meist öffentliche Netze	64.000 Baud	ISDN-Karte	
Com-Com	Analog über Telefonnetz	9.600 - 57.600 Baud je nach Netzqualität	Modem Digi-Board	
TCP / IP	Internet-Protokoll		Netzwerkkarte (DSL-)Modem	Service-Provider Firewall



1.2.1 ZVDFÜ

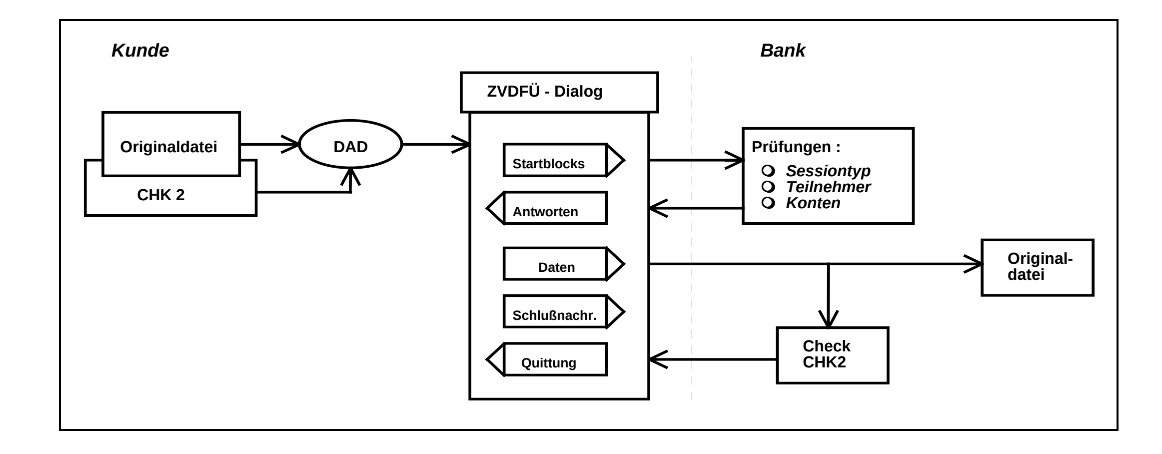
Das Kommunikationsverfahren ZVDFÜ wurde 1985 aufgrund der Anforderungen des ZKA entwickelt und enthält daher alle Merkmale, die dort zur Beschreibung eines sicheren DFÜ-Verfahrens aufgeführt sind.
Das Verfahren wurde permanent weiterentwickelt und z. B. um die Elektronische Unterschrift erweitert. In dieser Form wird das Verfahren als MCFT (**M**ulti**C**ash **F**ile **T**ransfer, s. Kapitel 1.2.2) bezeichnet und derzeit in Deutschland von ca. 50 Kreditinstituten eingesetzt. Darüber hinaus wird MCFT von vielen Banken in europäischen Ländern (Frankreich, Niederlande, Österreich, Polen, Rumänien, Russland, Schweiz, Slowakei, Spanien, Tschechien, Ungarn, usw.) genutzt. In Luxemburg wurde dieses Verfahren 1994 zum nationalen Standard bestimmt.

	ZVDFÜ
Merkmal	spezielles, auf die ZKA-Anforderungen zugeschnittenes Verfahren
Prüfung auf fehlerfreie Datenübertragung	ja
Komprimierung	ja (ZIP-Verfahren)
Verschlüsselung	Triple-DES mit asymmetrischem Schlüsselaustausch nach Diffie-Hellman
Formatvalidierung (syntaktische Prüfung)	während der Übertragung
Vorab-Autorisierungsprüfung	immer
Mitteilung des Prüfungsergebnisses	sofort am Ende der Übertragung
Autorisierung/ Manipulationsschutz	PRF2 direkte Prüfung (online)
EU	nein
Verteilte EU	nein
Kommunikationsmedien	Modem X.25 ISDN TCP/IP (Internet)
Einsatzbereich	Electronic Banking Europa

Beim ZVDFÜ-Verfahren (ZVDFÜ = Zahlungsverkehrsdatenfernübertragung) ist die Kommunikation zwischen Kunde und Bank aus Sicherheitsgründen in verschiedene Schritte unterteilt.
Es findet zwischen Bankrechner und Kundensystem ein Dialog statt.

Eine einfache Zusammenfassung dieser Schritte zeigt die nachfolgende Abbildung:

Datenaustausch mit ZVDFÜ





Die Dialogschritte im einzelnen:

- **Startnachricht**
  Nachdem die Verbindung zwischen Kunde und Bank hergestellt wurde, meldet sich der Kundenrechner über die Startnachricht beim Bankrechner an. Neben der Teilnehmernummer, dem Sessiontyp der zu übertragenden Datei, Bank-ID und Kontonummer ist ein wesentlicher Bestandteil der Startnachricht der KZV (**K**unden-**Z**ahlungs**V**erkehrsschlüssel).

  Der KZV ist ein dynamischer Schlüssel, der für jeden Teilnehmer individuell über das **Public-Key-Exchange**-Verfahren nach **Diffie/Hellman** berechnet wird. Eine erläuternde Abbildung zu diesem Verfahren befindet sich weiter unten in diesem Kapitel.
  Der Schlüssel selbst wird nicht übertragen, sondern bildet nur den Startwert zur späteren **KZVNEU-Berechnung**. Nur die errechnete Änderung des KZV wird an die empfangende Bank übertragen.

- **Antwortnachricht**
  Wird der Teilnehmer anhand der Startnachricht vom Bankrechner eindeutig identifiziert (Berechtigung für den zu übertragenden Sessiontyp, PIN usw.), erfolgt die Antwortnachricht des Bankrechners. Nur wenn die Antwortnachricht des Bankrechners vorliegt, beginnt die Übertragung der Daten.

- **DTA-Nachricht(en)**
  Die Zahlungsverkehrsdaten werden vor der Übertragung auf dem Kundenrechner verschlüsselt und komprimiert; die Entschlüsselung und Dekomprimierung erfolgt auf der Bankseite.

  Für die Komprimierung/Dekomprimierung von DTAUS- und DTAZV-Dateien wird ein speziell für das ZVDFÜ-Verfahren entwickelte Verfahren genutzt, das die Erstellung eines optimalen Komprimats gewährleistet. Für die Komprimierung/Dekomprimierung anderer Dateitypen (auch MT940-Dateien) wird PKZIP angewandt.

- **Schlussnachricht**
  Sind alle in einem Arbeitsgang zu übertragenen DTA-Nachrichten vom Kundenrechner an den Bankrechner übertragen worden, erhält der Bankrechner eine Information darüber, dass keine weiteren DTA-Nachrichten mehr folgen. Gleichzeitig wird dem Bankrechner die Prüfsumme über die übertragenen Daten mitgeteilt.
  Ebenfalls übertragen werden Antwort-Codes (vgl. Kapitel 5.4: *Antwort-Codes*), die den Status bzw. das Ergebnis der DFÜ beschreiben.

- **Quittungsnachricht**
  Wurden vom Bankrechner alle DTA-Nachrichten ohne Fehler empfangen und stimmt die vom Kundenrechner übermittelte Prüfsumme mit der vom Bankrechner errechneten überein, sendet dieser an den Kundenrechner eine Quittungsnachricht; damit ist der Übertragungsvorgang beendet. Auf Kunden- und Bankseite schließt sich die Neuberechnung des KZV (KZVNEU-Berechnung) an. Der neu berechnete KZV wird bei der nächsten Übertragung benötigt.

Beim KZV handelt es sich um einen symmetrischen Schlüssel, d. h. beide Kommunikationspartner (= Bank und Kunde) benutzen zum Verschlüsseln und Entschlüsseln einer Nachricht denselben Schlüssel.

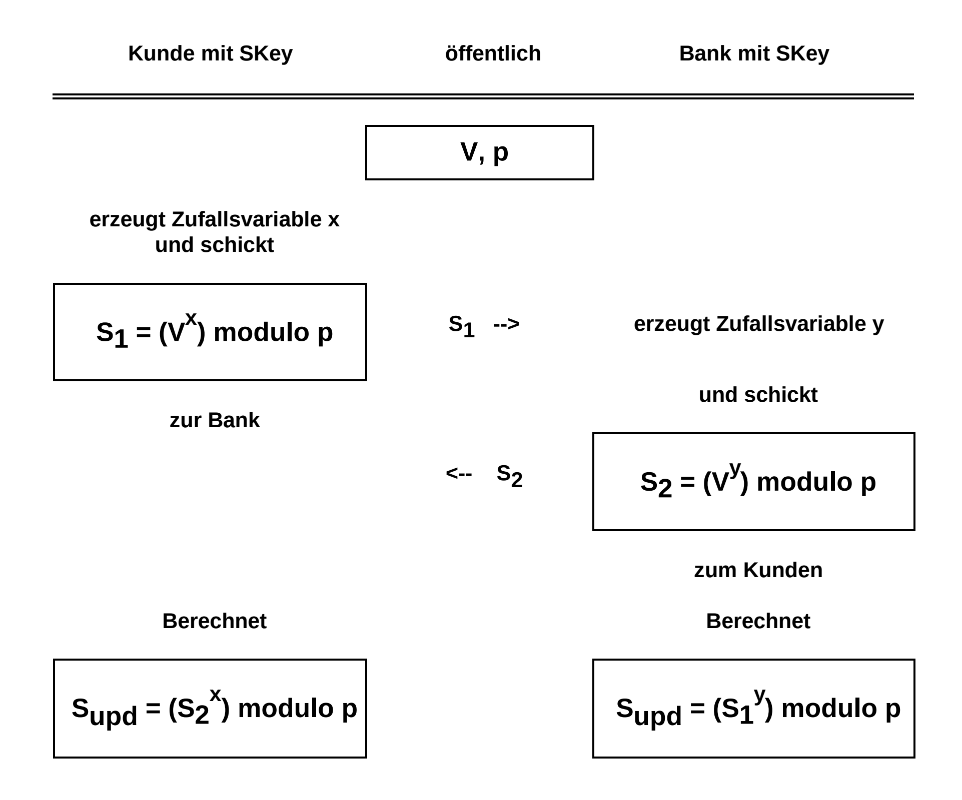
Durch den Schlüsselwechsel auf Bank- und Kundenseite nach jeder Übertragung ist eindeutig nachweisbar, mit welcher (teilnehmerorientierten) Bankparameterdatei die Übertragung durchgeführt wurde. Denn ein ordnungsgemäßer Datenaustausch kann nur stattfinden, wenn die Schlüssel identisch sind, d. h. jeder Kommunikationspartner die vereinbarten Schlüssel kennt.

Ein Nachweis darüber, welche Person (Mitarbeiter) mit der teilnehmerorientierten Bankparameterdatei Übertragungen durchführt, ist nicht möglich.

Gleichzeitig bildet dieser Schlüsselwechsel einen sicheren Schutz vor Manipulationen, da jeder Schlüssel nur einmal verwendet wird.



Schlüsselaustausch (Public-Key-Exchange) nach Diffie/Hellman



Von $\mathbf{S_1}$ und $\mathbf{S_2}$ kann **nicht** auf **x** und **y** geschlossen werden !
Es handelt sich um eine "**one-way-Funktion**".

Die Variable **V** und der Wert für die Moduloberechnung **p** sind allen Beteiligten zugänglich, d. h. sie sind öffentlich. Beide Zahlen sind Primzahlen und es gilt: $V < p$.

Der KUNDE erzeugt eine Zufallsvariable **x**. Die öffentliche Variable **V** wird mit der Zufallsvariable x potenziert und modulo p berechnet. Das Ergebnis dieser Berechnung, der Schlüssel $\mathbf{S_1}$, wird an die BANK übertragen.
Die BANK wiederum erzeugt eine Zufallsvariable **y**. Auch hier wird die öffentliche Variable **V** mit der Zufallsvariable y potenziert und modulo p berechnet. Das Ergebnis dieser Berechnung, der Schlüssel $\mathbf{S_2}$, wird an den KUNDEN übertragen.

Auf Kunden- wie auf Bankseite bilden die ausgetauschten Schlüssel $\mathbf{S_1}$ und $\mathbf{S_2}$ die Basis für die Berechnung des Schlüssel-Updates ($\mathbf{S_{upd}}$ bzw. KZVUpdate). Der S_{upd} wird mit dem vorhandenen Session Key (SKey) verknüpft und bildet so den neuen, für den nächste nachfolgende Übertragung zu verwendenden Schlüssel SKey (= Session Key).



1.2.2 MCFT

MCFT basiert auf dem Standard-Protokoll ZVDFÜ. Dieses Standard-Verfahren wurde um die Elektronische Unterschrift erweitert, sodass jetzt auch ein Nachweis darüber möglich ist, welche Person (Mitarbeiter) mit der teilnehmerorientierten Bankparameterdatei Datenübertragungen vorgenommen hat.

Alle anderen Merkmale, also auch Komprimierung und Verschlüsselung, entsprechen ZVDFÜ.

	MCFT
Merkmal	ZVDFÜ + EU
Prüfung auf fehlerfreie Datenübertragung	ja
Komprimierung	ja (ZIP-Verfahren)
Verschlüsselung	Triple-DES mit asymmetrischem Schlüsselaustausch nach Diffie-Hellman
Formatvalidierung (syntaktische Prüfung)	während der Übertragung
Vorab-Autorisierungsprüfung	immer
Mitteilung der Prüfungsergebnisse	sofort am Ende der Übertragung
Autorisierung / Manipulationsschutz	RSA-Unterschrift 1024 Bit RipeMD-160 direkte Prüfung (online)
EU	ja
Verteilte EU	ja
Kommunikationsmedien	Modem X.25 ISDN TCP / IP (Internet)
Einsatzbereich	Electronic Banking Europa

Zur Generierung der Elektronischen Unterschrift (EU) auf Kundenseite können die verschiedenen EU-Typen (ARL, SNI, Concord-Eracom, Omikron) mit der Ausprägung M000, M001 und M002 genutzt werden. Die Ausprägung bestimmt das Verfahren zur Berechnung des HASH-Wertes für die EU. Der jeweilige Bankrechner muss in der Lage sein, Elektronische Unterschriften, die mit allen EU-Typen in der Ausprägung M000, M001 und M002 erzeugt und per MCFT übertragen wurden, zu verifizieren.

Die HASH-Funktion generiert eine Prüfsumme über eine beliebig lange Datei (= Originaldatei). Der so ermittelte HASH-Wert dient als Grundlage für die Elektronische Unterschrift.

Die **Elektronische Unterschrift** basiert auf einem asymmetrischen Verschlüsselungsverfahren. Dabei nutzt jeder Kommunikationspartner ein aus Private Key (= geheimer Schlüssel) und Public Key (= Öffentlicher Schlüssel) bestehendes Schlüsselpaar (= Keypaar oder Key pair). Das bekannteste Public-Key-Verfahren ist **RSA**, so genannt nach seinen Entwicklern Rivest, Shamir und Adleman, das auch im Kunden- und Banksystem Anwendung findet.

Auf dem Kundenrechner wird durch das Zusatzmodul "EU" ein solches Schlüsselpaar generiert. Der öffentliche Teil des Schlüsselpaares wird dem Kommunikationspartner (der bzw. den Bank(en)) per DFÜ zur Verfügung gestellt; der Private Key dagegen wird auf einer per EU-Passwort zusätzlich gesicherten Diskette abgelegt. Werden Nachrichten zwischen den Kommunikationspartnern ausgetauscht, wird die vom Kundenrechner zu sendende Nachricht (= Zahlungsauftrag) mit dem Private Key verschlüsselt. Die empfangende Gegenstelle (Bank) entschlüsselt die Nachricht mit dem dazugehörigen, ihr übermittelten Public Key. Nur derjenige Kommunikationspartner kann eine Nachricht entschlüsseln, dem auch der zum Private Key passende Public Key vorliegt.



Der eigentlichen Übertragung von Zahlungsaufträgen ist der Versand eines **Startblocks** vorgelagert. Dieser Startblock enthält alle zur Prüfung erforderlichen Informationen, wie Kunden-ID, Teilnehmer-Nr., zu belastendes Konto, die Elektronische Unterschrift und Prüfsummen zur gesamten Datei sowie die TAN (transaction authentification number), die den Absender eines Auftrages eindeutig identifiziert. Dadurch ist es möglich, frühzeitig Fehler/Manipulationen festzustellen und die eigentliche Datenübertragung zu unterbinden.

Wird eine **Elektronische Unterschrift** per MCFT übermittelt, dann enthält der Startblock zusätzlich den "Fingerabdruck" zur Originaldatei und auch die Elektronische Unterschrift selbst. Dies hat den Vorteil, dass die Elektronische Unterschrift - sofern alle erforderlichen Unterschriften geleistet wurden - bereits während der Kommunikation verifiziert werden kann. Im Startblock können bis zu 6 Unterschriften übermittelt werden.

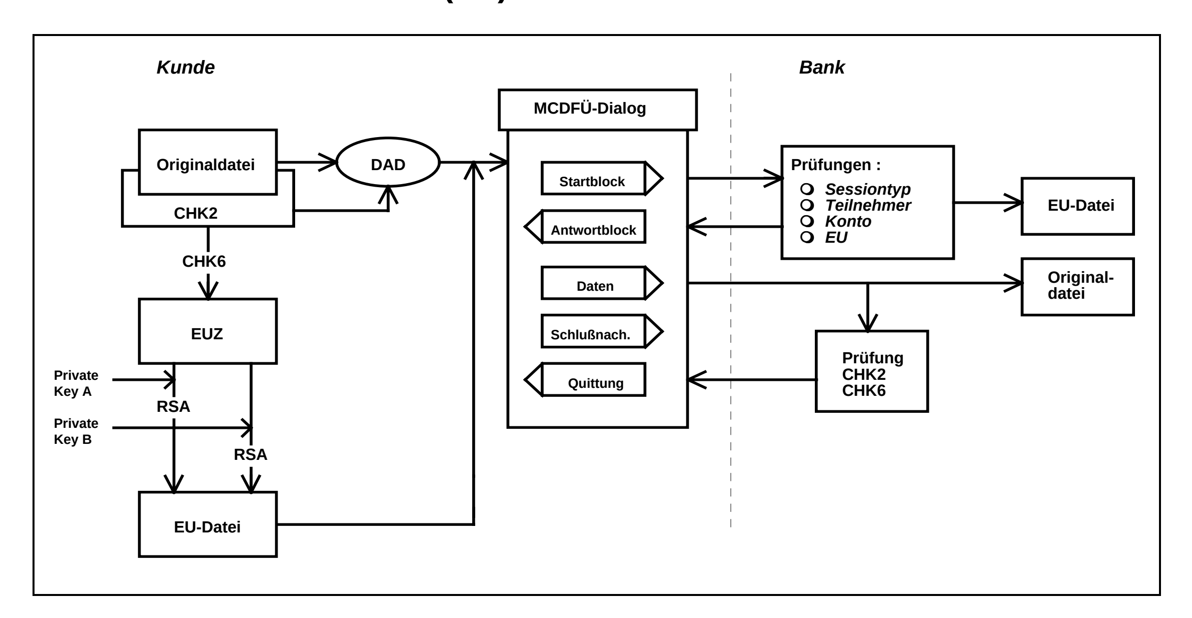
Ergibt die Prüfung auf der Bankseite, dass

- eine der im Startblock enthaltenen Unterschrift nicht korrekt ist, wird die DFÜ vor der Übertragung der Originaldatei abgebrochen.
- alle Unterschriften korrekt sind, wird die Originaldatei übertragen. Nach der Übertragung der Originaldatei wird auf Bankseite der "Fingerabdruck" nachgerechnet und mit demjenigen verglichen, der im Startblock mit übertragen und für korrekt befunden wurde. Ergibt die Nachberechnung des "Fingerabdrucks" eine Übereinstimmung mit den übertragenen Werten, wird dies dem Kundensystem im Schlussblock mit einem"OK" mitgeteilt.
  Stimmt der nachgerechnete "Fingerabdruck" nicht mit dem im Startblock übermittelten überein, wird die Originaldatei zurückgewiesen.

Schlussnachrichten werden entweder bei Beendigung der Kommunikation oder des Dialoges übermittelt.
Sie enthalten Antwort-Codes (vgl. Kapitel 5.4: *Antwort-Codes*), die den Status bzw. das Ergebnis der DFÜ beschreiben.
Die beim Kundensystem eingehenden Antwort-Codes werden dort ausgewertet und in den entsprechenden Protokollen angezeigt.



Elektronische Unterschrift (EU) mit MCFT



CHK2	=	Prüfsumme 2
CHK6	=	Prüfsumme 6
DAD	=	Kommunikationsauftrag
EUZ	=	EU-Zwischendatei
RSA	=	Verschlüsselungsverfahren nach Rivest, Shamir, Adleman

Über die Originaldatei wird ein HASH-Wert gebildet. Dieser HASH-Wert wird zusammen mit Datum und Uhrzeit der Generierung der Originaldatei, deren Namen usw. in die EUZ-Datei (= EU-Zwischen-Datei) eingestellt. Die EUZ-Datei wird mit dem Private Key "unterschrieben" und das Ergebnis dieser "Unterschriftsleistung" unter Angabe des Unterschriftsleistenden, Datum und Uhrzeit der Unterschrift, des verwendeten EU-Typs und der Ausprägung sowie weiteren Informationen in die EU-Datei eingestellt.



Verteilte Elektronische Unterschrift (EU) mit MCFT

Bank

Kunde 1
Originaldatei
CHK2
DAD
CHK6
EUZ
Private Key A
RSA
EU-Datei
MCDFÜ-Dialog
Startblock
Antwortblock
Daten
Schlußnachr.
Quittung
1. EU Prüfung
Originaldatei
Bereit für 2. bzw. n. EU
EU-Datei
vollständig ?
fehlerhaft ?
Protokoll

Kunde 1
MCDFÜ-Dialog

Kunde 2 / Kunde n
Originaldatei
DAD
CHK6
EUZ
Private Key B
RSA
EU-Datei
DAD
MCDFÜ-Dialog
Startblock
Antwortblock
Daten
Schlußnachr.
Quittung
Kunde 2 / Kunde n
Originaldatei oder DISP-Datei
MCDFÜ-Dialog
Startblock
Schlußnachr.
Quittung
2. bzw. n. EU-Prüfung

Kunde 2 / Kunde n
MCDFÜ-Dialog

CHK2 = Prüfsumme 2
CHK6 = Prüfsumme 6
DAD = Kommunikationsauftrag
DISP-Datei = Datei mit den wesentlichen, komprimierten Daten eines oder mehrerer Aufträge zum Anzeigen (DISP = DISPLAY)
EUZ = EU-Zwischendatei
RSA = Verschlüsselungsverfahren nach Rivest, Shamir, Adleman

Neben dem zuvor beschriebenen Verfahren ist es mit MCFT auch möglich, sog. "**verteilte Unterschriften**" zu leisten. Das Konzept einer "verteilten Unterschrift" sieht vor, das Unterschriftsberechtigte von unterschiedlichen Orten aus Unterschriften zu den beim Bankrechner hinterlegten Originaldateien leisten können. Das Verfahren der "verteilten Unterschrift" kann daher z. B. Unterschriftshierarchien in international tätigen Unternehmen abbilden, d. h. die Zielgruppe für den Einsatz der "verteilten Unterschrift" sind Firmenkunden mit mehrstufiger, räumlich getrennter Unternehmensstruktur (Konzerne, Filialbetriebe).



System		Aktion
Kundenrechner 1	+	Erstellung Zahlungsdatei
	+	Erstunterschrift
	+	Versand an Bank
Banksystem	x	Prüfung - *Zugangsberechtigung* - *Übertragungsberechtigung* - *Unterschrift* - *Ausreichende Anzahl Unterschriften*
	x	Online Rückmeldung - *Zahlung abgewiesen* oder - *Zahlung akzeptiert* oder - *Weiterleitung zur Zweitunterschrift*
	x	Datei bereitstellen für Zweit- bzw. n. Unterschrift
Kundenrechner 2 / n.	+	Abholen der Zahlungen zur Zweit- bzw. n. Unterschrift
	+	Zweit- bzw. n. Unterschrift
	+	Versand an Bank
Banksystem	x	Prüfung - *Zugangsberechtigung* - *Übertragungsberechtigung* - *Unterschrift* - *Ausreichende Anzahl Unterschriften*
	x	Online Rückmeldung - *Zahlung abgewiesen* oder - *Zahlung akzeptiert*
	x	Protokoll bereitstellen für Erstunterzeichner - *Zahlung abgewiesen* - *Zahlung akzeptiert* - *(Datei nach x Tagen mangels*
Zweitunterschrift gelöscht)		
Kundenrechner 1	+	Abholen Protokoll



1.2.3 FTAM

FTAM ist die Abkürzung für "File Transfer Access Method" und beschreibt ein Standardverfahren zum Austausch von Daten. Der nachfolgende Auszug aus der ZKA-Merkmal-Tabelle zeigt an, welche Anforderungen realisiert sind.

	FTAM
Merkmal	Kombination von Standardverfahren
Prüfung auf fehlerfreie Datenübertragung	nur mit EU
Komprimierung	FLAM (wahlweise)
Verschlüsselung	DES/RSA-Hybrid-Verfahren (wahlweise)
Formatvalidierung (syntaktische Prüfung)	nach der Übertragung
Vorab-Autorisierungsprüfung	nein
Mitteilung der Prüfungsergebnisse	später Prüfungsergebnis in Protokolldatei
Autorisierung / Manipulationsschutz	RSA-Unterschrift 1024 Bit RipeMD-160 getrennte Dateien Prüfung offline
EU	ja (wahlweise)
Verteilte EU	nein
Kommunikationsmedien	X.25 ISDN
Einsatzbereich	Electronic Banking Deutschland

Da hier verschiedene Standardverfahren (FTAM, FLAM (=Abkürzung für Frankenstein-Lidzba Access Method), EU) miteinander kombiniert wurden, ist ein Dialog - wie er in den DFÜ-Verfahren ZVDFÜ/MCFT realisiert wurde - nicht möglich. Insbesondere kann keine online-Prüfung der EU stattfinden.

Bei der derzeit realisierten Datenübertragung per FTAM handelt es sich um einen nationalen Standard.

Kennzeichen der FTAM-Übertragungen ist, dass die Daten bislang nicht verschlüsselt und nur wahlweise komprimiert, also transparent, zwischen den Kommunikationspartnern ausgetauscht werden. Zur Absicherung der übertragenen Daten ist unbedingt eine Elektronische Unterschrift erforderlich.

Bestandteil der per FTAM übertragenen Dateien ist ein interner Programmname (= OSI-FTAM-Name), anhand dessen Aufbau das Bank- und Kundensystem den Kommunikationspartner und den Dateityp identifiziert. Der interne Dateiname wird für jede Datei generiert.

Allgemein geschrieben lautet der interne Dateiname:

An.kkkkkkkk.aaa.dddNN.Annn{.pppp}



Die verwendeten Symbole haben folgende Bedeutung:

An Versionsnummer des Anwendungsprotokolls
n = **1**:bis BCS-Kundensoftware-Version 1.13
n = **2**: ab Version 1.20 (d. h. keine Bildung des Fingerprint2 im Rahmen der Elektronischen Unterschrift mehr)
n = **3**: ab Version 2.11 mit Verschlüsselung (d. h. Kundensystem unterstützt Verschlüsselung und das Verfahren des automatisierten BPD-Updates)

kkkkkkkk Kunden-ID (8 Stellen alphanumerisch)

aaa Auftragsart (3 Stellen alphanumerisch)
z. B. IZV, AZV, ...

dddNN Auftragsattribut (5 Stellen alphanumerisch)

1. Stelle : Dateiart:
   - B Originaldatei und EU-Datei in einer physikalischen Datei
   - D Originaldatei ohne Unterschrift
   - O Originaldatei, zu der eine Unterschriftsdatei benötigt wird
   - U Unterschriftsdatei
2. Stelle : Komprimierungsart:
   - N ohne Komprimierung
   - F mit FLAM-Komprimierung
   - X mit Xpress-Komprimierung (geplant)
3. Stelle : N ohne Verschlüsselung
   H mit Verschlüsselung (Hybrid-Verfahren DES)
4. Stelle : N z. Z. nicht belegt
5. Stelle : N z. Z. nicht belegt

Annn Auftragsnummer (4 Stellen alphanumerisch)

1. Stelle : A
2. Stelle : Kundenrechner-Identifikation im Netz beginnend mit A
3. und 4 Stelle : laufende Nummer (je Stelle 0 - 9, A - Z)

pppp ... Auftragsparameter (max. 50 Stellen alphanumerisch)

Auftragsart	**Auftragsparameter**
für nicht aktuelle Daten (z. B. STA)	optional Datum-von Datum-bis (VJJMMTT.BJJMMTT) Die Parameter geben den Zeitraum an, in dem sich die Daten befinden, die abgeholt werden sollen
VPK	Kennung für User-ID des Kunden, der VPK-Auftrag unterschrieben hat Byte 1: U (Kennung für User-ID) Byte 2-9: User-ID
alle verschlüsselt zu übertragenden	Verschlüsselungs-Public-Key- Hashwert (33 Bytes alphanumer.): Byte 1:H: (Kennung für Hashwert) Byte 2-33: Verschlüsselungs-Public-Key in Hex-Darstellung

Beispiel für einen komprimierten und verschlüsselten "Von-Bis"-STA-Auftrag:
A3.KUNDE1.STA.DFHNN.A001.V990814.B990815.H1A2B3C4E5112BCDEA7C81A2AB2782C



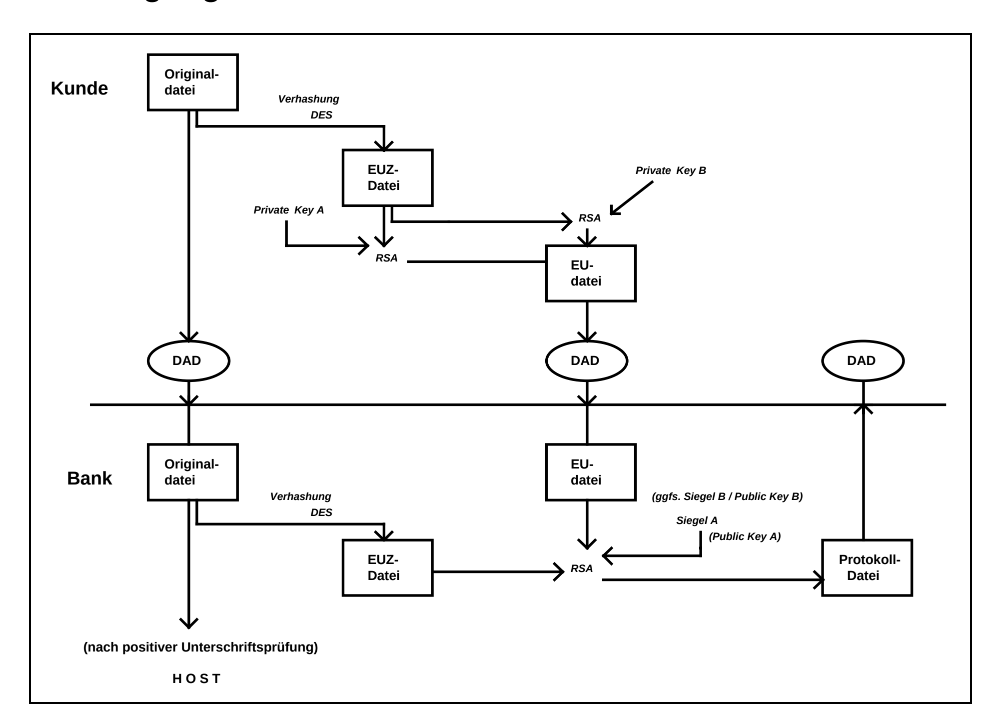
Beispiel für einen VPK-Auftrag mit Elektronischer Unterschrift:
A3.KUNDE1.VPK.BNNNN.A001.UUSER1

Für das Senden von Zahlungsaufträgen vom Kundenrechner zum Banksystem sind insgesamt drei Übertragungsvorgänge erforderlich, da zunächst Originaldatei und Unterschriftsdatei getrennt zum Bankrechner übergeben werden. Auf dem Bankrechner erfolgt eine Prüfung nach Richtigkeit und Vollständigkeit der zur Originaldatei gehörenden EU-Datei. Das Ergebnis der Prüfung wird in eine Protokolldatei eingestellt, die vom Kunden in einer gesonderten (= dritten) DFÜ-Session beim Banksystem abgeholt werden muss. Erst wenn das Protokoll (= EU-Protokoll) mit einer positiven Bestätigung vorliegt, kann der Kunde sicher sein, dass sein Zahlungsauftrag auch ausgeführt wurde. Bei fehlerhaften bzw. nicht vollständigen Unterschriften enthält das EU-Protokoll aussagekräftige Meldungen.

Zur Bedeutung spezieller Antwort-Codes, die den Status bzw. das Ergebnis der DFÜ beschreiben, siehe Kapitel 5.4: *Antwort-Codes*).

Zur Generierung der Elektronischen Unterschrift (EU) auf Kundenseite können die verschiedenen EU-Typen (ARL, SNI, Concord-Eracom, Omikron) genutzt werden. Im Gegensatz zu dem in MCFT angewendeten Verfahren stehen die einzelnen EU-Typen in den Ausprägungen A002, A003 und A004 zur Verfügung. Die Ausprägung bestimmt das Verfahren zur Berechnung des HASH-Wertes für die EU. Der jeweilige Bankrechner muss in der Lage sein, Elektronische Unterschriften, die mit allen EU-Typen in allen Ausprägungen erzeugt und per FTAM übertragen wurden, zu verifizieren.

Generierung und Prüfung der "Elektronischen Unterschrift" (EU) bei FTAM-Übertragungen



DAD	=	Kommunikationsauftrag
DES	=	Data Encryption Standard
EUZ	=	EU-Zwischendatei
RSA	=	Verschlüsselungsverfahren nach Rivest, Shamir, Adleman



Verschlüsselung der per FTAM übertragenen Dateien

Die wesentlichen Punkte des Konzeptes zur Verschlüsselung (vgl. Kapitel 4.5: *Verschlüsselung bei FTAM-/FTP-Übertragungen*) sind der Austausch von jeweils auf der Kunden- und Bankseite generierten Public Keys. Die beim Kunden bzw. bei der Bank verbleibenden Private Keys des Schlüsselpaares dienen zum Entschlüsseln der vom Kommunikationspartner mit dem jeweiligen Public Key verschlüsselten Nachrichten.

Zur Übertragung der Public Keys von der Bank zum Kunden bzw. vom Kunden zur Bank werden zwei Sessiontypen (Auftragsarten) genutzt, und zwar

VPB Verschlüsselungs-Public Key der Bank abholen
VPK Verschlüsselungs-Public Key (Kunde) senden

Die beiden (Verwaltungs-)Auftragsarten werden mit Hilfe eines entsprechenden Assistenten ausgeführt (s. Kapitel 4.5.1: *Verschlüsselung mit Banken in Betrieb nehmen*.

Die Verschlüsselung von per FTAM zu übertragenden Dateien arbeitet daher mit einem

- **Bankbezogenen Schlüsselpaar**
  (für die Verschlüsselung der zu sendenden Daten)
  - Generierung eines Keypaars auf der Bankseite
    (beliebig wiederholbar)
  - Abholen des **Public Keys** durch den Kunden
    (Sessiontyp **VPB**)
  - Ist der Public Key nicht mehr gültig,
    erfolgt Meldung durch die Bank und automatisches Initiieren einer neuen VPB-Session seitens des Kunden

sowie einem

- **Kundenbezogenen Schlüsselpaar**
  (Kunden-ID bezogen; Speicherung auf der Festplatte des Kunden)
  - Generierung eines Keypaars auf der Kundenseite
    (beliebig wiederholbar)
  - Übermittlung des **Public Keys** an alle (verschlüsselnden) Banken
    (Sessiontyp **VPK**)

Die zugehörigen Antwort-Codes bei Verschlüsselung finden Sie in Kapitel 4.5.2: *DFÜ-Returncodes im Rahmen der Verschlüsselung*.



Der Ablauf der vorbereitenden/nachbereitenden Schritte zur Übermittlung von verschlüsselten Daten per FTAM ist auf der nachfolgenden Abbildung schematisch dargestellt.

Übermittlung von verschlüsselten Daten mit FTAM

Kunde holt ab
Bank ist SENDER

Kunde überträgt
Kunde ist SENDER

MT940

DTAUS

Generierung DES-Schlüssel
beim SENDER

DES-Schlüssel = DEK = DES Key
in 3 Varianten : 40 Bit
64 Bit (Standard-DES)
128 Bit (Triple-DES)

Verschlüsselung der Datei
mit DEK (CBC-Mode)

Generierung des PDEK durch
Auffüllen mit führenden Nullen

PDEK = Padded DES Key
auf insgesamt 768 Bit

Verschlüsselung der PDEK
mit Public Key des Empfängers

über RSA bildet
EDEK = Encrypted DES Key

Vorsatz
MT940

Vorsatz
DTAUS

D F Ü

mit Übermittlung des
Hash-Wertes des Public Keys
im Remote-Namen

Prüfung

nicht OK

OK

Aufforderung
- VPB abholen
- VPK senden

Entschlüsselung

EDEK mit Private Key => PDEK
(Nur der berechtigte Empfänger kann entschlüsseln.)

Entfernen

Entfernen der padding-Information => DEK

Entschlüsselung

DEK

Originaldatei



1.2.4 FTP

FTP ist die Abkürzung für "File Transfer Protocol" und beschreibt ein Standardverfahren zum Austausch von Daten auf TCP/IP-Basis. Die nachfolgende Merkmal-Tabelle zeigt an, welche Anforderungen realisiert sind.

	FTP
Merkmal	Kombination von Standardverfahren
Prüfung auf fehlerfreie Datenübertragung	ja
Komprimierung	FLAM (wahlweise)
Verschlüsselung	DES/RSA-Hybrid-Verfahren
Formatvalidierung (syntaktische Prüfung)	nach der Übertragung
Vorab-Autorisierungsprüfung	optional
Mitteilung des Prüfungsergebnisses	sofort bzw. später (Prüfungsergebnis in Protokolldatei)
Autorisierung / Manipulationsschutz	RSA-Unterschrift 1024 Bit RipeMD-160 optional: Vorabprüfung (online) ausführliche Prüfung: offline
EU	ja (wahlweise)
Verteilte EU	ja
Kommunikationsmedien	TCP/IP (Internet)
Einsatzbereich	Electronic Banking deutsche Privatbanken

Für die Abwicklung eines FTP-Auftrages wird ein (interner) Dateiname definiert, anhand dessen sowohl das Bank- als auch das Kundensystem den Kommunikationspartner und den Dateityp identifizieren. Dieser Dateiname wird für jede Datei generiert.

Allgemein geschrieben lautet der interne Dateiname:

`B1.kkkkkkkk.aaa.dddNN.Annn`

Die verwendeten Symbole haben folgende Bedeutung:

`B1` Versionsnummer des Anwendungsprotokolls

`kkkkkkkk` Kunden-ID (8 Stellen alphanumerisch)

`aaa` Auftragsart (3 Stellen alphanumerisch)
z. B. IZV, AZV, ...

`dddNN` Auftragsattribut (5 Stellen alphanumerisch)

1. Stelle : Dateiart:
   - D Datei ohne Unterschrift
   - O Originaldatei, zu der eine Unterschriftsdatei benötigt wird
   - I Infodatei zu D oder O
   - S Infodatei mit EU zu O

2. Stelle : Komprimierungsart:



			N	ohne Komprimierung
			F	mit FLAM-Komprimierung
			X	mit Xpress-Komprimierung (geplant)
	3. Stelle	:	N	ohne Verschlüsselung
			H	mit Verschlüsselung (Hybrid-Verfahren DES)
	4. Stelle	:	N	z. Z. nicht belegt
	5. Stelle	:	N	z. Z. nicht belegt

Annn Auftragsnummer (4 Stellen alphanumerisch)

1. Stelle	:	A
2. Stelle	:	Kundenrechner-Identifikation im Netz beginnend mit A
3. und 4 Stelle	:	laufende Nummer (je Stelle 0 - 9, A - Z)

Ein FTP-DFÜ-Auftrag setzt sich aus mindestens zwei, in der Regel jedoch aus drei Dateitypen zusammen:

- der Login-Datei zur Legitimation/Anmeldung
- der Informationsdatei zur Spezifizierung des Auftrags, ggf. mit EU
- der Nutzdatendatei (die entfallen kann, wenn nur die EU übertragen werden soll)

Für das Senden von Zahlungsaufträgen vom Kundenrechner zum Banksystem werden bei einem DFÜ-Auftrag insgesamt drei Übertragungsvorgänge durchgeführt: zuerst für die Login-Datei, dann für die Informationsdatei und schließlich für die Originaldatei (Nutzdatendatei). Auf dem Bankrechner erfolgt eine Prüfung nach Richtigkeit und Vollständigkeit der zur Originaldatei gehörenden EU. Das Ergebnis der Prüfung wird in eine Protokolldatei eingestellt, die vom Kunden in einem gesonderten DFÜ-Auftrag beim Banksystem abgeholt werden muss. Erst wenn das Protokoll (= EU-Protokoll) mit einer positiven Bestätigung vorliegt, kann der Kunde sicher sein, dass sein Zahlungsauftrag auch ausgeführt wurde. Bei fehlerhaften bzw. nicht vollständigen Unterschriften enthält das EU-Protokoll aussagekräftige Meldungen.

Zur Bedeutung spezieller Antwort-Codes, die den Status bzw. das Ergebnis der DFÜ beschreiben, siehe Kapitel 5.4: *Antwort-Codes*).

Zur Generierung der Elektronischen Unterschrift (EU) auf Kundenseite können die verschiedenen EU-Typen (ARL, SNI, Concord-Eracom, Omikron) genutzt werden. Die Ausprägung bestimmt das Verfahren zur Berechnung des HASH-Wertes für die EU.

Der Ablauf der vorbereitenden/nachbereitenden Schritte zur Übermittlung verschlüsselter Daten per FTP entspricht dem Verfahren zur Übertragung von verschlüselten Daten via FTAM-Prozess (siehe Kapitel 1.2.3: *FTAM*). Auch hier erfolgt die Verschlüsselung (vgl. Kapitel 4.5: *Verschlüsselung bei FTAM-/FTP-Übertragungen*) über den Austausch von jeweils auf der Kunden- und Bankseite generierten Public Keys. Die beiden (Verwaltungs-)Auftragsarten VPB und VPK werden mit Hilfe eines entsprechenden Assistenten ausgeführt (s. Kapitel 4.5.1: *Verschlüsselung mit Banken in Betrieb nehmen*).
Im Gegensatz zum FTAM-Prozess werden die Daten bei der Datenfernübertragung mittels FTP allerdings **generell in verschlüsselter Form** versandt. Die einzige Ausnahme bildet das Abholen des Verschlüsselungs-Public-Keys der Bank (VPB) durch den Kunden, der für die Verschlüsselung der zu übertragenden Dateien erforderlich ist. Danach werden alle Dateien des Kunden und der Bank nur noch verschlüsselt übermittelt.
Die zugehörigen Antwort-Codes bei Verschlüsselung finden Sie in Kapitel 4.5.2: *DFÜ-Returncodes im Rahmen der Verschlüsselung*.



Zusätzlich ist es mit FTP auch möglich, sogenannte **Verteilte Elektronische Unterschriften (VEU)** zu leisten. Das Konzept einer "Verteilten Elektronischen Unterschrift" sieht vor, dass Unterschriftsberechtigte von unterschiedlichen Orten aus Unterschriften zu den beim Bankrechner hinterlegten Originaldateien leisten können (vgl. Kapitel 1.2.2: *MCFT*).

Das Verfahren der Verteilten Elektronischen Unterschrift kann daher z. B. Unterschriftshierarchien in international tätigen Unternehmen abbilden, d. h. die Zielgruppe für den Einsatz der verteilten Unterschrift sind Firmenkunden mit mehrstufiger, räumlich getrennter Unternehmensstruktur (Konzerne, Filialbetriebe).

Ablauf einer Verteilten Elektronischen Unterschrift beim FTP-Prozess:

1. Kunden, die bankseitig für die Verteilte Elektronische Unterschrift vorgesehen sind, können diese initialisieren, indem Sie eine nicht vollständig unterschriebene Originaldatei an die Bank übertragen. Zusätzlich zu dieser Originaldatei gibt der Kunde im Anhang der zum Auftrag gehörenden Informationsdatei an, welche Kunden weitere Elektronische Unterschriften für diesen Auftrag zu leisten haben. Überdies kann auf der Bankseite eine Liste hinterlegt werden, in der die Kunden aufgeführt werden, die für weitere Elektronische Unterschriften vorgesehen sind. Gibt der Kunde im Auftrag keine mitunterschreibenden Kunden an, so werden die für die Unterschriftsleistung benötigten Dateien gemäß den Angaben in der Verteilerliste weitergeleitet.

2. Die Bank stellt die Unterschriftsdaten in Form von ESG-Dateien (**E**lectronic **S**ignature **G**et) für die Kunden zur Abholung bereit, die durch den die VEU initiierenden Kunden vorgegeben wurden. Die Unterschriftsdaten bestehen aus dem Hashwert in Verbindung mit der Displaydatei oder der gesamten Originaldatei. Diese Daten werden von der Bank allerdings nur dann zur Abholung bereitgestellt, wenn die Elektronische Unterschrift des initiierenden Kunden für die Originaldatei vorliegt und erfolgreich geprüft wurde. Erhält die Bank von **einem** Kunden mehrere zu unterschreibende Aufträge, so wird die ESG-Datei fortgeschrieben, d. h. die ESG-Datei enthält in solchen Fällen mehrere zu unterschreibende Aufträge.

3. Die ESG-Datei wird durch einen Teilnehmer abgeholt, der zur Ausführung der Auftragsart "ESG" autorisiert ist. Die bei der Bank abgeholte ESG-Datei wird auf Kundenseite während des Einlesevorgangs im Datei-Manager gegebenenfalls automatisch in die Einzelaufträge aufgeteilt.

4. Abgeschlossen wird der Vorgang durch die Generierung und die Übertragung einer weiteren elektronischen Unterschrift durch einen Teilnehmer, der über eine Unterschriftsberechtigung bei der betreffenden Bank verfügt.

5. Die Schritte 3 und 4 müssen jeweils wiederholt werden, bis bei der Bank eine ausreichende Unterzeichnung der Originaldatei gemäß den Unterschriftsberechtigungen der an dem Vorgang beteiligten Teilnehmern vorliegt.

Die Originaldatei wird durch den die VEU initiierenden Kunden **stets** mit Elektronischer Unterschrift übertragen, denn nur auf diese Weise kann der Inhalt der Originaldatei authentifiziert werden. Da der Teilnehmer des Kunden, der die VEU initiiert, auf der Bankseite nicht zwangsläufig über eine Unterschriftsberechtigung (Einzel-, Erst- oder Zweitunterschriftsberechtigung) verfügen muss, gibt es für solche Teilnehmer eine zusätzliche Unterschriftsklasse. Diese Unterschriftsklasse "T" wird ausschließlich zur Transportsicherung der Originaldatei verwendet. Bei einer Elektronischen Unterschrift der Klasse "T" finden nur die eigentliche EU-Prüfung sowie die Doppeleinreichungskontrolle statt, Kontoberechtigungs- und Höchstbetragsprüfungen entfallen.



1.2.5 EBICS

Das internetbasierte DFÜ-Verfahren EBICS (**E**lectronic **B**anking **I**nternet **C**ommunication **S**tandard) wurde im Auftrag des Zentralen Kreditausschusses (ZKA), dem Zusammenschluss aller Spitzenverbände des deutschen Bankgewerbes, definiert und soll das für das Firmenkundengeschäft der Kreditinstitute eingesetzte Kommunikationsverfahren FTAM ersetzen. Als wichtigste Erweiterung gegenüber FTAM ist die Unterstützung der "Verteilten Elektronischen Unterschrift", die eine gemeinsame Autorisierung von Zahlungen von unterschiedlichen Orten aus ermöglicht, sowie die *grundsätzlich verschlüsselte* Übertragung der Daten zwischen Kunde und Bank zu sehen. Aufgrund seiner hohen Performance eignet sich das EBICS-Verfahren insbesondere für die Abwicklung von Massenzahlungen.

Die neue EBICS-Version 2.4 ist die erste gemeinsame Initiative der deutschen und französischen Bankenverbände und muss von den Banken in beiden Ländern ab Herbst 2009 unterstützt werden.
Für Frankreich gibt es nur wenige Abweichungen zu der bisherigen Handhabung (Ersatz von ETEBAC-3). In der ersten Phase werden dort z. B. zunächst nur Transport-Signaturen, aber keine personenbezogenen Elektronischen Unterschriften für die Autorisierung von Zahlungsaufträgen unterstützt. Spezielle Auftragsarten ermöglichen das Hochladen (FUL: **F**ile **U**p**l**oad) und Herunterladen (FDL: **F**ile **D**own**l**oad) von Dateien mit zugehörigem Dateitypkennzeichen für allgemeine und bankspezifische Formate.
Die entscheidende Neuerung für Deutschland ist die erhöhte Sicherheit durch Unterstützung von längeren Signatur-Schlüsseln (neue EBICS-Protokollversion H003 mit EU-Versionen A005 und A006 [existieren nebeneinander]). Bei einer Neugenerierung der Schlüssel werden auch neue EBICS-Schlüssel der Versionen X002 und E002 generiert.

Mit der EBICS-Version 2.5 wird die Protokollversion H004 unterstützt. Nach der Umschaltung auf diese Protokollversion werden die Auftragsnummern für Sendeaufträge nicht mehr vom Clientsystem, sondern vom Bankserver vergeben.
Mit EBICS 2.5 kann alternativ zur bekannten Auftragsart PTK mit der Auftragsart HAC ein Kundenprotokoll im XML-Format abgerufen werden. Dies wird ebenfalls dem zugehörigen Dateimanagereintrag zugeordnet und zur Anzeige analog PTK aufbereitet.

Die nachfolgende Merkmal-Tabelle zeigt an, welche Anforderungen realisiert sind.

	EBICS
Merkmal	Internet
Prüfung auf fehlerfreie Datenübertragung	ja
Komprimierung	ja (ZIP-Verfahren)
Verschlüsselung	TLS (SSL) und DES/RSA-Hybridverfahren
Formatvalidierung (syntaktische Prüfung)	nach der Übertragung
Vorab-Autorisierungsprüfung	optional
Mitteilung der Prüfungsergebnisse	später im Protokoll
Autorisierung / Manipulationsschutz	RSA-Unterschrift 1024 Bit (ab 2.4: 1536-4096 Bit, Standard: 2048) RipeMD-160 (ab 2.4: SHA: 256) optional: Vorab-Prüfung (online) ausführliche Prüfung: offline
EU	ja
Verteilte EU	ja
Kommunikationsmedien	TCP / IP (Internet)
Einsatzbereich	Electronic Banking Deutschland



Die Merkmale im Detail:

- EBICS ist IP-fähig und nutzt zur Datenübertragung das Internet-Transportprotokoll HTTPS, das mit der TLS (SSL)-Transportverschlüsselung eine sichere Übertragung gewährleistet.
Die in einen XML-Container eingebetteten Anwendungsdaten werden blockweise übertragen, wobei jeder Block über eine Authentifikationssignatur (Authentifikationsschlüssel ab Version X001) abgesichert wird. Werden nicht alle Blöcke erfolgreich übertragen, ermöglicht eine Recovery-Funktion das Anknüpfen an den zuletzt erfolgreich übertragenen Block.

- Zusätzlich zur Transportsicherung wird durch die integrierte Verschlüsselung (Verschlüsselungsschlüssel ab Version E001) nach dem BCS-Hybridverfahren sichergestellt, dass die Anwendungsdaten immer verschlüsselt übertragen werden (somit doppelte Verschlüsselung).

- Um die Authentizität der zu übertragenden Dateien zu gewährleisten, müssen diese vom Anwender stets mittels Elektronischer Unterschrift (EU) autorisiert werden (Signaturschlüssel ab Version A004).

- Für eine effiziente Übertragung werden die Daten immer mit einem ZIP-Algorithmus komprimiert.

- EBICS unterstützt zudem den Einsatz der Verteilten Elektronischen Unterschrift (VEU), was es den Unternehmen ermöglicht, Zahlungsaufträge von verschiedenen Standorten aus autorisieren zu lassen.

Im Kapitel 3.5: *EBICS* finden Sie Informationen zu den notwendigen Einstellungen in der zugehörigen Bankparameterdatei.

Die Funktionalität der Verteilten Elektronischen Unterschrift (VEU) bedeutet, dass Unterschriften von räumlich getrennten Kundensystemen nur durch Kommunikation mit dem jeweiligen Banksystem geleistet werden können. Dies ist auf dem Banksystem pro Kunde konfigurierbar.

Die Verteilte Elektronische Unterschrift erlaubt es, Aufträge orts- und zeitunabhängig von mehreren Teilnehmern – auch kundenübergreifend – zu autorisieren. Ein zugrunde liegender Auftrag bleibt hierbei in der VEU-Prozessverarbeitung gespeichert, bis über die VEU-Aufträge entweder die erforderliche Anzahl Unterschriften mit der passenden Berechtigung eingegangen sind, ein bankrechnerseitiges Zeitlimit überschritten wurde oder ein Auftragsstorno erfolgt.



Ablaufdiagramm der Verteilten Elektronischen Unterschrift bei EBICS:

Auftraggeber/ Einreicher
Kreditinstitut
Unterzeichner
neuer Auftrag
[weitere EUs benötigt]
[EU-Berechtg. vollständig]
Löschen des Auftrags aus VEU-Prozessverarb.
Speicherung des Auftrags in VEU-Prozessverarb.
HVU
[keine Aufträge zu sig.]
[Aufträge zur Sig. vorh.]
Ausführung des Auftrags
HVD
[HVT wird unterstützt]
[komplette Auftragsdatei gewünscht]
HVT (komplette Auftragsdatei)
[Auftragsdetails gewünscht]
[HVT wird nicht unterstützt]
HVT (Auftragsdetails)
[Auftrags-Hashwert aus HVD]
[Hashwert aus Auftragsdatei berechnet]
Löschen des Auftrags aus VEU-Prozessverarb.
HVS
[Storno]
[Sig. des Auftrags]
HVE
[keine Sig.]

Ein Teilnehmer stößt die VEU-Prozessverarbeitung an, indem er einen Auftrag mit einer unzureichenden Anzahl bankfachlicher Unterschriften der benötigten Berechtigungsklassen einreicht. Es ist zwingend erforderlich ,dass dieser Auftrag signiert eingereicht wird (entweder mit bankfachlicher Unterschrift der Klassen "A", "B" oder "E" oder mit Transportunterschrift = Unterschriftsklasse "T").

Das Banksystem verifiziert zunächst die mitgelieferte(n) EU(s) und die Autorisation des Teilnehmers für die gegebene Auftragsart. Dann gleicht es die Anzahl und Unterschriftsklassen der gelieferten EU(s) mit den lokal hinterlegten EU-Anforderungen für die gegebene Auftragsart ab. Falls noch Unterschriften ausstehend sind, wird der Auftrag mitsamt den bereits übermittelten EUs in die VEU-Prozessverarbeitung eingestellt und somit für berechtigte Kunden zur VEU gespeichert.

Die einzelnen EBICS-Requests werden in der Applikationsebene zusammengefasst und mit den bereits bekannten Auftragsarten für die VEU abgewickelt:

ESG (Elektronische Zweitunterschrift abholen); diese Auftragsart kapselt die beiden EBICS-Requests:
- HVU (VEU-Übersicht abholen)
- HVD (VEU-Status abrufen)

ESP (Elektronische Zweitunterschrift senden); diese Auftragsart kapselt die EBICS-Requests:
- HVT (VEU-Transaktionsdetails abrufen)
- mehrere HVE (VEU-Unterschrift hinzufügen)
- HVS (VEU-Storno)



Der Teilnehmer holt im ersten Schritt eine Übersicht, für welche Aufträge er für die VEU unterschriftsberechtigt ist, bei der Bank ab (Auftragsart HVU). Im zweiten Schritt wird dann pro Auftrag der Status abgerufen (Auftragsart HVD). Dieser Abruf enthält für einen Auftrag im Wesentlichen den Hashwert des Originalauftrages, den Begleitzettel sowie die User, die bereits Unterschriften für diesen Auftrag geleistet haben. Diese beiden Schritte werden im Programm gekapselt, so dass der Teilnehmer dann nicht nach dem HVU-Abruf für jeden einzelnen Auftrag den HVD-Abruf manuell starten muss.

Die einzelnen Aufträge werden nach dem Abruf in den Dateimanager mit dem Status "Wartet auf EU" eingestellt. Darüber hinaus wird zur Kennzeichnung von VEU-Aufträgen ein neuer Ordnungsbegriff ("VEU") für diese Aufträge vergeben.

Bei einem HVU-/HVD-Abruf verfährt das Programm mit bereits im Dateimanager vorhandenen VEU-Aufträgen wie folgt:

1. VEU-Auftrag wurde noch nicht bearbeitet (Kein Teilnehmer hat eine Unterschrift geleistet; Status = "Wartet auf EU")

   Diese Aufträge werden im Dateimanager überschrieben. Sofern solche Aufträge noch bankseitig offen sind, liefert der HVU-/HVD-Abruf die entsprechende Information nochmals. Durch das Überschreiben wird vermieden, dass für einen identischen VEU-Auftrag mehrere Einträge im Dateimanager erzeugt werden.

2. VEU-Auftrag ist in Bearbeitung, aber noch nicht vollständig abgeschlossen (Teilnehmer hat eine Unterschrift geleistet, aber die Abfrage auf vollständige Unterschriften verneint; Status = "Wartet auf EU")

   Solche Aufträge bleiben im Dateimanager erhalten und werden nicht überschrieben, da diese noch nicht abgeschlossen sind. Es wird kein weiterer Eintrag für diesen Auftrag im Dateimanager erzeugt. Neue Informationen aus dem HVD-Abruf (z. B. Liste der bereits zu diesem Auftrag geleisteten Unterschriften) werden dem vorhandenen Eintrag hinzugefügt.

3. VEU-Auftrag ist in Bearbeitung, aber noch nicht vollständig abgeschlossen (Teilnehmer hat Unterschrift geleistet, aber noch nicht zur Bank übertragen; Status = "Wartet auf DFÜ")

   Solche Aufträge bleiben im Dateimanager erhalten und werden nicht überschrieben, da diese noch nicht abgeschlossen sind. Es wird kein weiterer Eintrag für diesen Auftrag im Dateimanager erzeugt. Neue Informationen aus dem HVD-Abruf werden dem vorhandenen Eintrag hinzugefügt. Der Status wird nicht umgesetzt, da die bereits geleistete, aber noch nicht verschickte Unterschrift die letzte Notwendige sein kann. Der Teilnehmer kann so seine geleistete EU sofort verschicken.

4. VEU-Auftrag ist in Bearbeitung, aber noch nicht vollständig abgeschlossen (Teilnehmer hat Unterschrift geleistet und zur Bank übertragen, aber das Protokoll mit abschließender EU-Prüfung wurde noch nicht abgeholt; Status = "OK")

   Solche Aufträge bleiben im Dateimanager erhalten, da diese noch nicht abgeschlossen sind. Neue Informationen aus dem HVD-Abruf werden dem vorhandenen Eintrag hinzugefügt. In diesem Fall wird der Status des Auftrages auf "Wartet auf EU" zurückgestellt, damit weitere Teilnehmer Unterschriften hinzufügen können.

5. VEU-Auftrag ist vollständig abgeschlossen (Teilnehmer hat Unterschrift geleistet und zur Bank übertragen; Protokoll mit abschließender EU-Prüfung wurde abgeholt). Der Status wird auf "EU-Prüfung OK" gesetzt.

Erfolgt ein Protokollabruf zu einem wartenden VEU-Auftrag wird der Status folgendermaßen gesetzt:
Ist der Auftrag auf Bankseite noch offen, erfolgt keine Statusänderung
Ist der Auftrag auf Bankseite inzwischen erfolgreich verarbeitet, weil ihn ein andere User unterschrieben hat, wir der Status auf "EU-Prüfung OK" gesetzt.

Solche Aufträge bleiben im Dateimanager als Nachweis zur Auftragsdurchführung erhalten.



Die Informationen aus dem Kundenprotokoll (Ergebnis der Unterschriftsprüfung) werden den Aufträgen im Dateimanager zugeordnet. Zur Identifikation des Auftrages wird hierzu die Kunden-ID, die User-ID sowie die Auftragsnummern (Auftragsnummer Einreichung Originaldatei, Auftragsnummer des Auftrages zur Leistung einer weiteren Unterschrift mittels HVE) herangezogen.

Für den HVT-Abruf kann für das Abholen der Originaldatei auf dem Bankrechner eine Grenze für die Dateigröße eingestellt werden.



1.2.6 HBCI/HBCI+

Das Verfahren HBCI (= Homebanking Computer Interface) sollte das bestehende BTX-Verfahren ersetzen. Der vom Zentralen Kreditauschuss der deutschen Kreditwirtschaft (ZKA) erstmals 1996 in der Version 1.0 verabschiedete HBCI-Standard erlaubt dank der Verwendung moderner kryptographischer Funktionen und der Nutzung von Chipkarten eine sichere Kommunikation über offene Netzte wie das Internet.

Mittlerweile (2003) wurde mit der HBCI-Version 3.0 der übergreifende Standard FinTS (Financial Transaction Services) geschaffen, der einerseits HBCI 3.0 und andererseits PIN/TAN als alternatives Sicherheitsverfahren enthält.

Beim HBCI+-Verfahren wird auf den HBCI-Standard zurückgegriffen, die Absicherung erfolgt jedoch wie bei BTX über PIN und TAN. Gegenüber dem früheren BTX stehen allerdings zeitgemäße Banking-Funktionen wie z. B. die EU-Standardüberweisung zur Verfügung. Das Verfahren ist gegenüber dem Verfahren mit Chipkarte standortunabhängig.

Die nachfolgende Tabelle zeigt die Unterschiede der beiden heute verfügbaren HBCI-Ausprägungen.

	HBCI	**HBCI+**
Merkmal	HBCI mit Chipkarte/Diskette	auch als HBCI Plus, HBCI mit PIN /TAN oder PIN/TAN erweitert bezeichnet
Prüfung auf fehlerfreie Datenübertragung	TCP / IP	TCP / IP
Komprimierung	ja	ja
Verschlüsselung	ja	ja 128-Bit-SSL (Browser)
Validierung (syntaktische Prüfung)	nein	nein
Autorisierung / Manipulationsschutz	EU RipeMD / RSA	PIN/TAN
Verteilte EU	nein	nein
Kommunikationsmedien	TCP / IP (Internet)	TCP / IP (Internet)
Einsatzbereiche	HomeBanking	HomeBanking



1.2.7 ETEBAC

ETEBAC (= *Echange télématique entre banques et clients*) ist das von französische Banken benutzte DFÜ-Verfahren. Es handelt sich hierbei um einen nationalen Standard, der vom AFB (*Association Française de Banques*) - dem Verband der französischen Banken - definiert ist.

Bei ETEBAC gibt es unterschiedliche Ausprägungen: ETEBAC3 und ETEBAC5. Für jede Ausprägung müssen entsprechende Zusatzmodule installiert werden. Bitte nehmen Sie Kontakt mit Ihrem Bankberater auf, falls Sie mit französischen Banken mit diesem Verfahren Daten austauschen möchten.

Im Kapitel 3.8: *ETEBAC3* finden Sie detaillierte Anleitungen zur Benutzung des ETEBAC3-Moduls.



Inhaltsverzeichnis: Kapitel 2

Seite



2 Menü Kommunikation

Im Menü -Kommunikation- sind sämtliche Menüpunkte gebündelt, die die Kommunikation zwischen Kunden- und Banksystem, d. h. die die Datenfernübertragung betreffen.

Folgende Menüpunkte sind im Menü -Kommunikation- zu finden:

- **Datei-Manager**
  Informationen zum Datei-Manager finden Sie in Kapitel 5.1: *Datei-Manager*.
- **DFÜ-Favorit ausführen**
  Informationen zum Ausführen bevorzugter Bankverbindungen finden Sie in Kapitel 5.1.1: *Datenbankübersicht Datei-Manager*.
- **Assistent Abholen von Daten bei mehreren Banken**
- **Monatsstatistik (Zusatzmodul)**

- **DFÜ-Parameter**
  Zur Durchführung einer ordnungsgemäßen DFÜ ist die korrekte Konfiguration der entsprechenden DFÜ-Parameter unerlässlich. Über die DFÜ-Parameter wird festgelegt, welche Einstellung je DFÜ-Einrichtung (z. B. ISDN oder X25) genutzt werden soll.
- **Bankparameterdateien**
  Eine Bankparameterdatei beschreibt den Zugang zu einer Bank. Sie benötigen pro Bank eine eigene Bankparameterdatei. Jede BPD enthält die Zugangsdaten zur jeweiligen Bank sowie die NUA (Network User Adress = "Telefonnummer"), unter der Sie Ihre Bank per DFÜ erreichen können.
  Bei der Erzeugung eines DFÜ-Auftrages wird die gewünschte Bank immer in Form einer Bankparameterdatei ausgewählt.

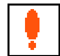
- **Erstinitialisierung**
- **EU-Schlüsselpaar generieren / versenden**
- **EU-Passwort ändern**
- **DFÜ-Passwort ändern**
- **EBICS-DFÜ-Passwort ändern**
- **Schlüsselmedien verwalten**
- **Zertifikate verwalten (Zusatzmodul)**

- **FTAM-/FTP-Bankzugang auf EBICS umstellen**
- **EBICS-Authentifikationsschlüssel austauschen**
- **Zurücksetzen eines ZVDFÜ-/MCFT-Zugangs**
- **FTAM-/FTP-Verschlüsselung**
  Dieser Menüpunkt ist nur nach einer Installation der DFÜ-Verfahren FTAM oder FTP verfügbar. Nähere Informationen zum Thema Verschlüsselung finden Sie in Kapitel 4.5: *Verschlüsselung*.
- **Sperren eines DFÜ-Zugangs**



2.1 DFÜ-Parameter

Zur Durchführung einer ordnungsgemäßen Datenfernübertragung ist die Konfiguration verschiedener DFÜ-Parameter in Abhängigkeit des jeweiligen DFÜ-Verfahrens notwendig. Selbstverständlich müssen nur die von Ihnen genutzten DFÜ-Verfahren durch Anpassen der entsprechenden DFÜ-Parameter konfiguriert werden.


Zur Konfiguration der DFÜ-Parameter halten Sie bitte alle Unterlagen (Modembeschreibungen, Passworte, Kennungen usw.) und Handbücher bereit. Hilfestellung bietet auch der Serviceberater Ihrer Bank.

Folgende DFÜ-Verfahren werden zur Zeit unterstützt:

- Modem-PAD-Zugang
- X.25 - Hauptanschluss
- Modem-Modem-Verbindung
- ISDN CAPI
- TCP/IP-Verbindung (Internet)

Über die entsprechenden Reiter können Sie Registerkarten aufrufen, deren Eingabefelder mit den für dieses DFÜ-Verfahren gültigen Standardwerten vorbelegt sind.

Nach Auswahl des DFÜ-Verfahrens und ggf. Konfiguration der jeweiligen DFÜ-Parameter teilen Sie dem Programm über die *Registerkarte Prioritäten* mit, welches DFÜ-Verfahren in welcher Reihenfolge genutzt werden soll.

In den DFÜ-Parametern werden die lokalen Informationen für die Kommunikation festgelegt. Da für die Datenfernübertragung spezielle Hardware angesprochen werden muss, werden diese Einstellungen je Rechner im Netzwerk verwaltet. Sollen mehrere Rechner mit den Banken kommunizieren, so müssen die DFÜ-Parameter auf jedem Rechner gepflegt werden. Nur Rechner mit gesetzten DFÜ-Parametern werden in der Applikation zur Kommunikation angeboten.

Eine Ausnahme bildet das Protokoll TCP/IP, das die Verbindung meist über die Standard-Netzwerkkarte herstellt. Daher kann hierfür auf der *Registerkarte Prioritäten* definiert werden, dass die TCP/IP-Parameter global gelten sollen. In diesem Fall muss TCP/IP nur einmalig auf einem beliebigen Rechner aktiviert und die Proxy-Parameter ebenfalls nur einmal eingetragen werden. Sie werden dann von allen Rechnern im Netzwerk verwendet.

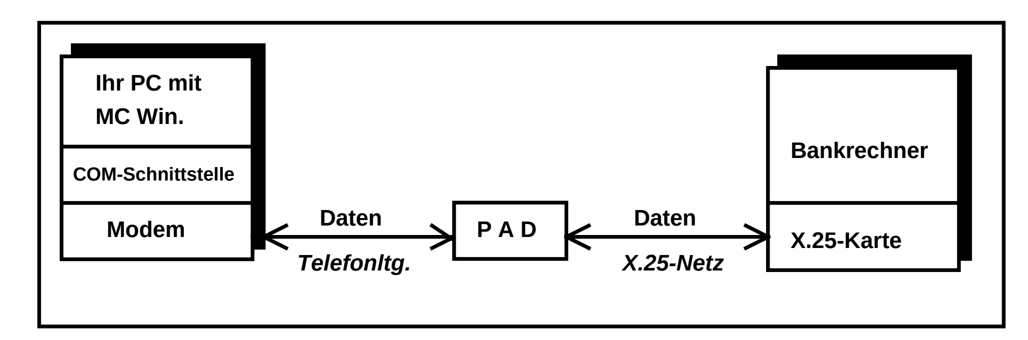
Bestätigen Sie schließlich Ihre Angaben mit [***Speichern***].



2.2 Registerkarte Modem-PAD-Zugang

Bei Nutzung dieses DFÜ-Verfahrens benötigen Sie eine freie COM-Schnittstelle in Verbindung mit einem externen Modem oder eine integrierte Modemkarte sowie einen Telefonanschluss. Die Kommunikation mit den verschiedenen Banken erfolgt über einem PAD (= Abkürzung für "**P**acket **A**ssembly / **D**isassembly" = Bezeichnung für einen Konzentrator, der Datenpakete z. B. im Datex-P-Betrieb (Deutschland) zusammenstellt bzw. trennt).

Der Verlauf der Kommunikation lässt sich anhand der folgenden Grafik verdeutlichen:



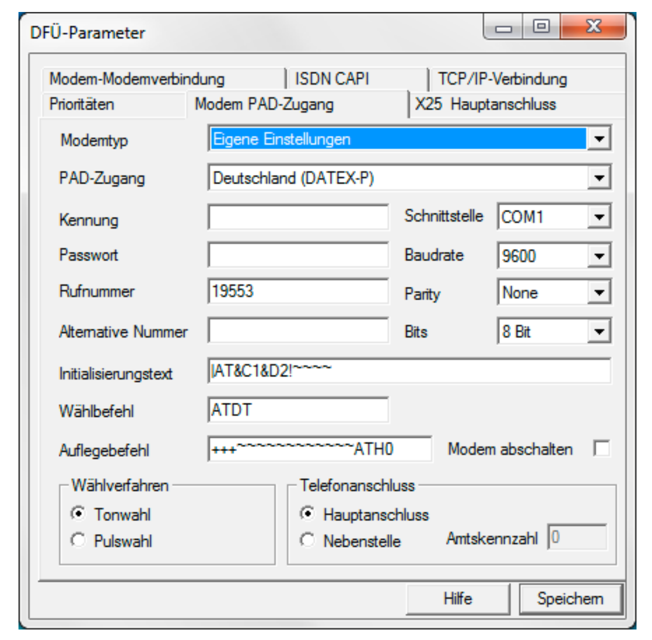
Die Eingabefelder der Dialogbox sind mit Einstellungen für eine Datenübertragung mit einem Standard-Modem vorbelegt. Die nicht ausgefüllten Felder müssen mit für Ihren Anschluss gültigen Werten gefüllt werden.

Falls Sie kein Standard-Modem verwenden, müssen die Einstellungen entsprechend des von Ihnen eingesetzten Modems angepasst werden. Hinweise zur Konfiguration finden Sie in der Dokumentation Ihres Modems.

Es stehen folgende Felder zur Verfügung:

Modemtyp

Wählen Sie aus der Liste das Modem aus, dass Sie bei den Windows-Systemeinstellungen unter Modem eingerichtet haben (Einstellungen werden übernommen) oder wählen Sie "Eigene Einstellungen".





PAD-Zugang

Wählen Sie aus der Liste der möglichen PAD-Zugänge den länder- bzw. bankspezifischen Zugang, den Sie nutzen wollen.

Kennung
Passwort

Diese beiden Felder nehmen die Datex-Kennung und das Datex-Passwort auf. Das Passwort ist bei der Eingabe verdeckt. Die eingegebenen Zeichen werden jeweils als ***** (Sternchen) dargestellt.

Kennung und Passwort wurden Ihnen von Ihrem Telekommmunikations-Dienstleister mitgeteilt.

Nummer

Zur Konfiguration einer automatischen Anwahl des nächsten PAD-Knotens muss das Feld "Nummer" (des nächsten PAD-Knotens) ausgefüllt werden.

Alternative Nummer

Sie haben die Möglichkeit, als Ergänzung zu der in erster Linie zu nutzenden PAD-Nummer (Nummer des PAD-Knotens) im Feld "**Alternative Nummer**" eine zweite Rufnummer einzutragen. Ist eine solche Rufnummer vorhanden, so wird diese im Besetztfall der ersten Nummer genutzt.

Schnittstelle

Bei der zu nutzenden Schnittstelle zwischen PC und Modem wählen Sie zwischen den seriellen Schnittstellen COM1, COM2, ..., COM8.

Baudrate

Die Baudrate bezieht sich auf die Geschwindigkeit, mit der Daten übertragen werden können. Die Baudrate ist abhängig von der Leistungsfähigkeit Ihres Modems. Die Standardeinstellung lautet auf "2400"; sie können jedoch Baudraten von "300" bis "64000" einstellen.

Parity

Die Parity-Angabe bezieht sich auf die Anforderungen, die der PAD an die Parität stellt. Bei der Paritätskontrolle (parity check) wählen Sie zwischen:

- even (gerade Parität) oder
- none (keine Parität).

Bits

Dieses Feld bestimmt, ob die Übertragung im 7-Bit- oder 8-Bit-Modus erfolgt. Welchen Modus Sie festlegen, ist abhängig von den Anforderungen, die der PAD an den Übertragungsmodus stellt.

Initialisierungstext

Zur Modem-Initialisierung werden bestimmte Befehle benötigt. Diese Befehle gehören in der Regel zum **AT-Befehlssatz**, der zu einem Quasi-Standard geworden ist. Es gibt jedoch bei den am Markt erhältlichen Modems gewisse Unterschiede in Art und Umfang des AT-Befehlssatzes. Ferner müssen bei einigen Modems AT-Befehle ausschließlich in Großbuchstaben eingegeben werden. Weitere Erläuterungen hierzu finden Sie in Kapitel 2.8: *AT-Befehle*.

Wählbefehl

Zur Konfiguration einer automatischen Anwahl des nächsten Datex-Knotens muss das Feld "Wählbefehl" ausgefüllt werden.

Der **Wählbefehl** wird entsprechend Ihren Angaben automatisch eingetragen.

Aufbau des Wählbefehls: **ATDabb**



Die einzelnen Buchstaben sind wie folgt zu ersetzen:

a = "T" bei Telefonanschlüssen mit Tonwahl
"P" bei Telefonanschlüssen mit Pulswahl

b = Amtsholung.
Bei hausinternen Anschlüssen (Nebenstelle) muss hier ggf. eine Amtsholung mit "0W" vorgenommen werden, wobei die "0" für die entsprechende Ziffer steht, die diese Funktion auslöst. Das "W" bedeutet "Warten, bis die Amtsleitung vorhanden ist".

Erläuterungen zum AT-Befehlssatz finden Sie in Kapitel 2.8: *AT-Befehle*.

Auflegebefehl

In dieses Feld tragen Sie ein, mit welchem Befehl die Verbindung zwischen Modem und PAD beendet werden soll.

Modem abschalten

Standardmäßig ist das Feld nicht aktiviert.

Lassen Sie das Feld unmarkiert, so bleibt beim Abarbeiten der verschiedenen DFÜ-Aufträge die Verbindung zum PAD bestehen. Nach Durchführung eines DFÜ-Auftrages wird bei einem Wechsel der anzuwählenden Bank lediglich die Verbindung zur bisherigen Bank aufgehoben. Im Anschluss wird sofort eine Verbindung zur nächsten Bank hergestellt, so dass duch Vermeidung einer kompletten Neuanwahl Kosten eingespart werden können.

Nach Auswahl dieses Feldes legt das Modem dagegen nach **jeder** Datenübertragung wieder auf, so dass bei Durchführung weiterer DFÜ-Aufträge vor Anwahl der jeweiligen Bank zunächst wieder eine Verbindung zum PAD hergestellt werden muss.
In Abhängigkeit vom anzuwählenden PAD kann dieses kostenintensive Verfahren allerdings erforderlich sein.

Wählverfahren

Wählen Sie, ob Ihr Modem Tonwahl oder Pulswahl unterstützt.

Telefonanschluss

Hier geben Sie an, ob es sich bei dem verwendeten Telefonanschluss um einen Hauptanschluss oder um eine Nebenstelle handelt. Eine gegebenenfalls notwendige Amtskennzahl können Sie in das entsprechende Feld eingeben.

Bei einer nachträglichen manuellen Änderung wird das Feld "Wählbefehl" entsprechend angepasst.

Auswahl	Feld "Wählbefehl"	Ergänzung Feld "Wählbefehl"
Tonwahl	ATDT	-
Pulswahl	ATDP	-
Hauptanschluss	-	-
Nebenstelle	-	0W
Amtskennzahl (x)	-	(x)W

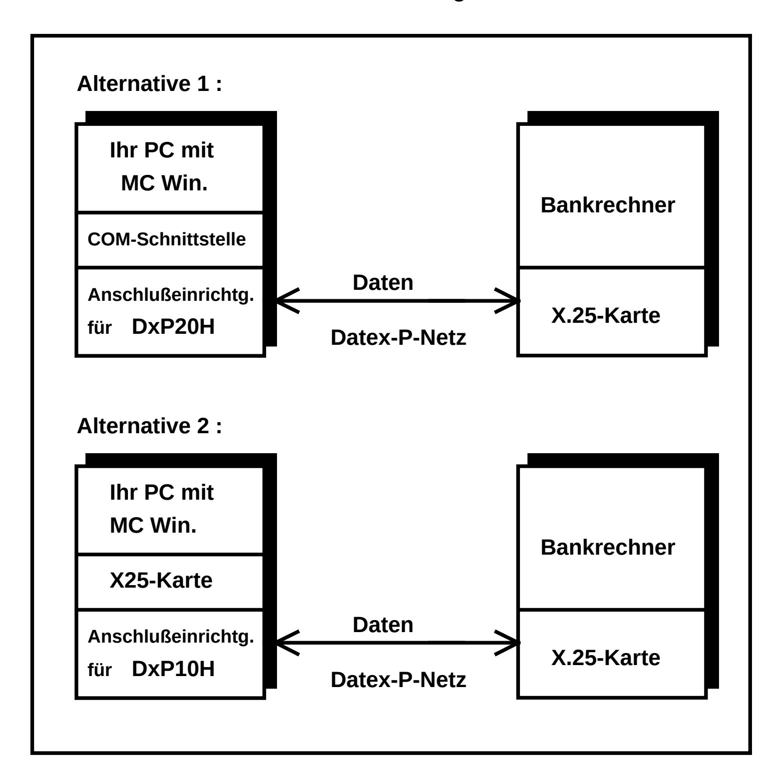


2.3 Registerkarte X.25 - Hauptanschluss

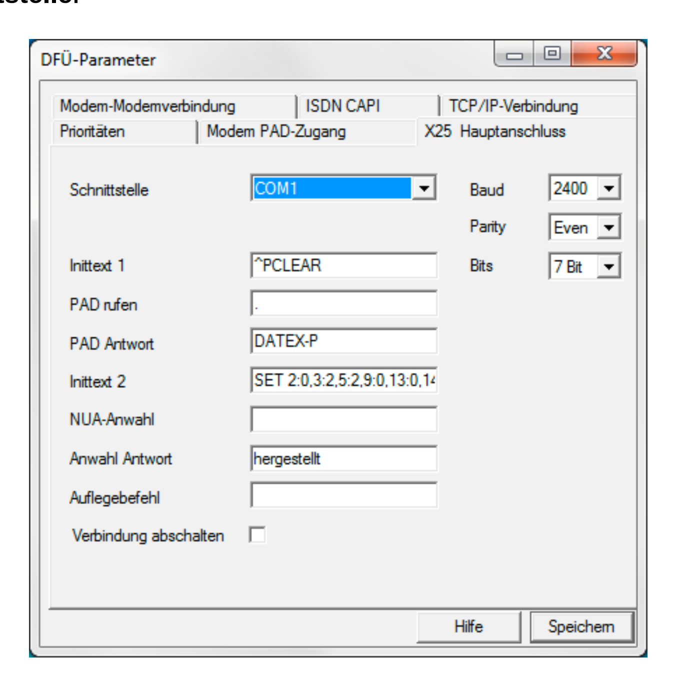
Bei Einsatz dieses DFÜ-Verfahrens benötigen Sie

entweder eine freie COM-Schnittstelle und einen Datex-P20-Hauptanschluss mit entsprechender Anschlusseinrichtung der Telekom
oder eine X.25-Karte und einen Datex-P10-Hauptanschluss mit entsprechender Anschlusseinrichtung der Telekom.

Der Verlauf der Kommunikation lässt sich anhand der folgenden Grafik verdeutlichen:



Der Aufbau der Registerkarte, die Sie durch Anklicken des Reiters aufrufen, ist abhängig von der zu verwendenden **Schnittstelle**.





X.25

Wenn Sie als Übertragungseinrichtung "X.25" festgelegt haben, müssen Sie über einen Datex-P10-Hauptanschluss verfügen und die Kartentreiber **VOR** dem Start von Windows laden.
Eine weitere Konfiguration ist in diesem Fall nicht notwendig.

COM1 bis COM8

Die Übertragungsparameter müssen ggf. dem installierten Modem angepasst werden. Hinweise zu den zu verwendenden Parametern finden Sie in der Dokumentation zur genutzten DFÜ-Peripherie.

Die Felder der Maske haben folgende Bedeutung:

Baud

Die Baudrate bezieht sich auf die Geschwindigkeit, mit der Daten übertragen werden können. Die Baudrate ist abhängig von der Leistungsfähigkeit Ihres Modems. Die Standardeinstellung lautet auf "2400"; sie können jedoch Baudraten von "300" bis "64000" einstellen.

Parity

Bei der Paritätskontrolle (parity check) wählen Sie zwischen:

- even (gerade Parität) oder
- none (keine Parität)

Bits

Dieses Feld bestimmt, ob die Übertragung im 7-Bit- oder 8-Bit-Modus erfolgt.

Inittext 1

Der Initialisierungstext 1 ist abhängig vom zu verwendenden Modem. Hinweise zu den entsprechenden Befehlen entnehmen Sie bitte der Dokumentation Ihres Modems.

PAD rufen
PAD Antwort

Über die Belegung des ersten Feldes wird dem PAD mitgeteilt, dass eine Übertragung erfolgen soll. Durch eine Rückantwort des PAD wird dem Programm mitgeteilt, dass der Verbindungsaufbau erfolgreich durchgeführt wurde. Die unter "PAD rufen" und "PAD Antwort" einzutragenden Werte sind abhängig vom PAD.

Bei Nutzung der Telekom-PADs gilt:

Standard bei **PAD rufen** ist ein **.** (Punkt).
Standard für die Rückmeldung des PAD (= **PAD Antwort**) ist "**DATEX-P**".

Inittext 2

Der Initialisierungstext 2 ist wie der Inittext 1 abhängig vom zu verwendenden Modem. Hinweise zu den entsprechenden Befehlen entnehmen Sie bitte der Dokumentation Ihres Modems.

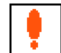
NUA-Anwahl

Die **NUA** (**N**etwork **U**ser **A**dress) ist die "Telefonnummer", unter der spezielle (auch ausländische) PADs per DFÜ erreichbar sind. Der PAD-Betreiber teilt Ihnen mit, welche Eintragung hier vorzunehmen ist.

Die NUA-Anwahl ist **abhängig** vom jeweiligen **PAD**.

Tragen Sie die Ihnen mitgeteilte NUA **OHNE** Leerzeichen zwischen den einzelnen Ziffern in das Eingabefeld ein.




Bei Nutzung der Telekom-PADs bleibt das Feld leer.

Anwahl Antwort

In das Feld "Anwahl Antwort" tragen Sie die Zeichenkette ein, die beim Aufbau einer DFÜ-Verbindung an die Gegenstelle gesendet werden soll. Die Antwort zeigt der Gegenstelle an, dass die Verbindung von nun an besteht. Dieses Feld ist **abhängig** vom **PAD.**

Bei Nutzung der Telekom-PADs gilt:

Standard für die Anwahl Antwort ist "**hergestellt**".

Auflegebefehl

Hier teilen Sie dem Programm mit, mit welchem Befehl die Verbindung zwischen Modem und PAD gelöst werden soll.

Verbindung abschalten

Bei Auswahl dieses Feldes wird die Verbindung nach erfolgter Datenübertragung automatisch aufgehoben. Im anderen Fall müssen Sie selbst tätig werden, um die Verbindung (evtl. zu einem erheblich späteren Zeitpunkt) zu beenden.

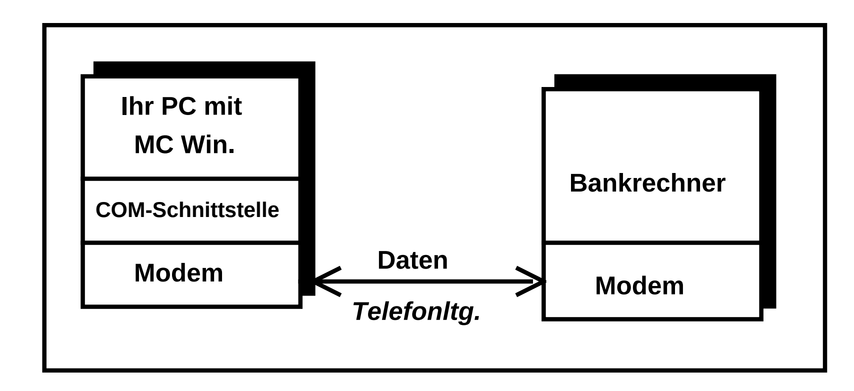
Die Einstellung -**Nein**- bietet jedoch einen Kostenvorteil, da beim Abarbeiten von Auftragsdateien, die Aufträge für unterschiedliche Banken enthält, die Verbindung zum PAD bestehen bleibt.
In diesem Fall muss bei Durchführung weiterer DFÜ-Aufträge vor Anwahl der jeweiligen Bank nicht wieder eine Verbindung zum PAD hergestellt werden.



2.4 Registerkarte Modem-Modem-Verbindung

Bei Nutzung dieses DFÜ-Verfahrens benötigen Sie eine freie COM-Schnittstelle in Verbindung mit einem externen Modem oder eine integrierte Modemkarte sowie einen Telefonanschluss.

Der Verlauf der Kommunikation lässt sich anhand der folgenden Grafik verdeutlichen:



Die Eingabe von Parametern für eine Modemverbindung ist nur dann erforderlich, wenn die Bank, mit der Sie Daten austauschen wollen, nur die Verbindungsart "Modem <---> Modem" anbietet.

Die Eingabefelder der Dialogbox sind mit Einstellungen für eine Datenübertragung mit einem Standard-Modem vorbelegt. Die nicht ausgefüllten Felder müssen mit für Ihren Anschluss gültigen Werten gefüllt werden.

Falls Sie kein Standard-Modem verwenden, müssen die Einstellungen entsprechend des von Ihnen eingesetzten Modems angepasst werden. Hinweise zur Konfiguration finden Sie in der Dokumentation Ihres Modems.

Es stehen folgende Felder zur Verfügung:

Modemtyp

Wählen Sie aus der Liste das Modem aus, dass Sie bei den Windows-Systemeinstellungen unter Modem eingerichtet haben (Einstellungen werden übernommen) oder wählen Sie "Eigene Einstellungen".

Schnittstelle

Bei der zu nutzenden Schnittstelle zwischen PC und Modem wählen Sie zwischen den seriellen Schnittstellen COM1, ..., COM8.

Baudrate

Die Baudrate bezieht sich auf die Geschwindigkeit, mit der Daten übertragen werden können. Die Baudrate ist abhängig von der Leistungsfähigkeit Ihres Modems. Die Standardeinstellung lautet auf "2400"; sie können jedoch Baudraten von "300" bis "64000" einstellen.

Parity

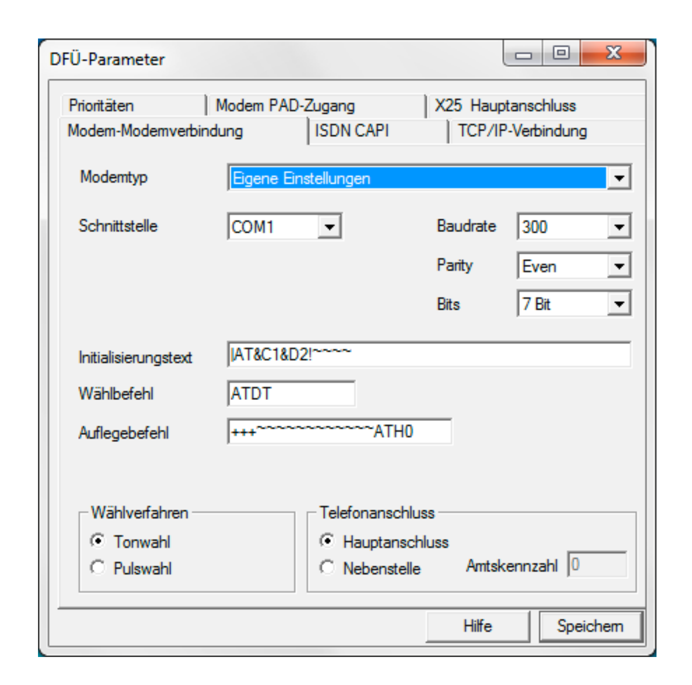
Die Parity-Angabe bezieht sich auf die Anforderungen, die der PAD an die Parität stellt. Bei der Paritätskontrolle (parity check) wählen Sie zwischen:

- even (gerade Parität) oder
- none (keine Parität).

Bits

Dieses Feld bestimmt, ob die Übertragung im 7-Bit- oder 8-Bit-Modus erfolgt.





Initialisierungstext

Zur Modem-Initialisierung werden bestimmte Befehle benötigt. Diese Befehle gehören in der Regel zum **AT-Befehlssatz,** der zu einem Quasi-Standard geworden ist. Es gibt jedoch bei den am Markt erhältlichen Modems gewisse Unterschiede in Art und Umfang des AT-Befehlssatzes. Ferner müssen bei einigen Modems die Befehle ausschließlich in Großbuchstaben eingegeben werden. Weitere Erläuterungen hierzu finden Sie in Kapitel 2.8: *AT-Befehle*.

Wählbefehl

Zur Konfiguration einer automatischen Anwahl des nächsten Datex-Knotens muss das Feld "Wählbefehl" ausgefüllt werden.

Der **Wählbefehl** wird entsprechend Ihren Angaben automatisch eingetragen.

Aufbau des Wählbefehls: **ATDabb**

Die einzelnen Buchstaben sind wie folgt zu ersetzen:

a = "T" ist Telefonanschlüssen mit Tonwahl
"P" ist Telefonanschlüssen mit Pulswahl

b = Amtsholung.
Bei hausinternen Anschlüssen (Nebenstelle) muss hier ggf. eine "Amtsholung" mit "0W" vorgenommen werden, wobei die "0" für die entsprechende Ziffer steht, die diese Funktion auslöst. Das "W" bedeutet "Warten, bis die Amtsleitung vorhanden ist".

Erläuterungen zum AT-Befehlssatz finden Sie in Kapitel 2.8*: AT-Befehle*.

Auflegebefehl

In dieses Feld tragen Sie ein, mit welchem Befehl die Verbindung zwischen Ihrem und dem Bank-Modem beendet werden soll.

Wählverfahren

Wählen Sie, ob Ihr Modem Tonwahl oder Pulswahl unterstützt.

Telefonanschluss

Hier geben Sie an, ob es sich bei dem verwendeten Telefonanschluss um einen Hauptanschluss oder um eine Nebenstelle handelt. Eine gegebenenfalls notwendige Amtskennzahl können Sie in das entsprechende Feld eingeben.



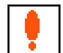
Bei einer nachträglichen manuellen Änderung wird das Feld "Wählbefehl" entsprechend angepasst.

Auswahl	Feld "Wählbefehl"	Ergänzung Feld "Wählbefehl"
Tonwahl	ATDT	-
Pulswahl	ATDP	-
Hauptanschluss	-	-
Nebenstelle	-	0W
Amtskennzahl (x)	-	(x)W



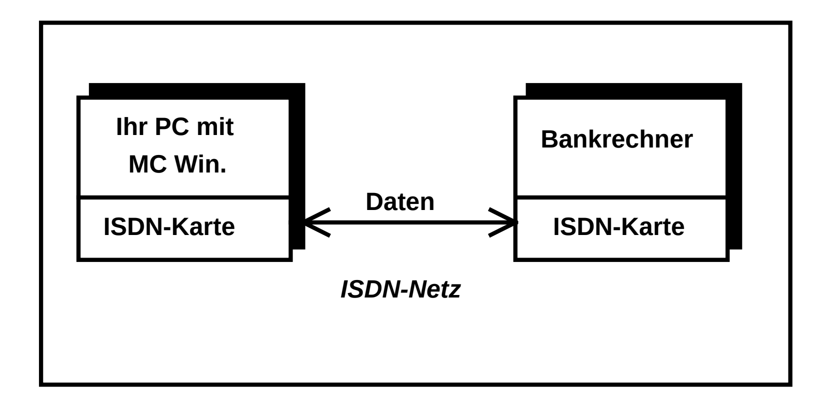
2.5 Registerkarte ISDN CAPI

Bei Nutzung dieses DFÜ-Verfahrens benötigen Sie eine ISDN-Karte sowie einen von der Telekom installierten ISDN-Anschluss. Ausserdem muss Ihr Kreditinstitut in der Lage sein, über ISDN Daten zu empfangen bzw. zu versenden.



Die von Ihnen verwendete ISDN-Karte muss entsprechend den Vorgaben des Herstellers konfiguriert werden. Informationen dazu finden Sie in der mitgelieferten Dokumentation der ISDN-Karte.Darüber hinaus müssen die Treiber der ISDN-Karte auf jeden Fall **VOR** dem Start von Windows geladen werden.

Der Verlauf der Kommunikation lässt sich anhand der folgenden Grafik verdeutlichen:



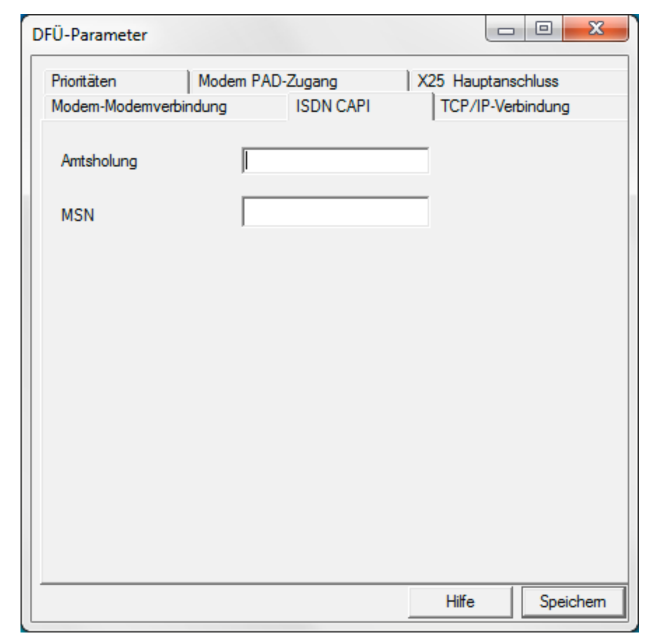
Die folgenden Parameter stehen bei Verwendung von ISDN zur Verfügung:

Amtsholung

Bei hausinternen Anschlüssen (Nebenstelle) muss hier ggf. eine Amtsholung mit "0W" vorgenommen werden, wobei die "0" für die entsprechende Ziffer steht, die diese Funktion auslöst.

MSN (Mehrfachrufnummer beim EURO-ISDN)

Tragen Sie hier die Ihrem Endgerät zugeordnete, bis zu 6 Ziffern umfassende Mehrfachnummer ein.

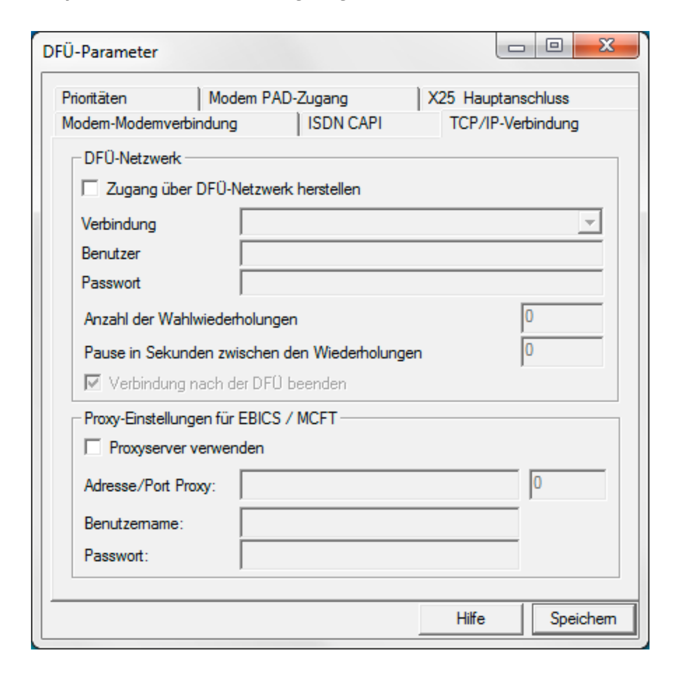




2.6 Registerkarte TCP/IP-Verbindung

Bietet eine Ihrer Banken den Datenaustausch über das Internet unter Nutzung der DFÜ-Verfahren ZVDFÜ, MCFT, FTP oder EBICS an (vgl. Kapitel 3.2: *ZVDFÜ/MCFT*, 3.4: *FTP*) bzw. 3.5: *EBICS*), so aktivieren Sie auf der *Registerkarte Prioritäten* das Feld "TCP/IP-Verbindung".

Voraussetzung für den Datenaustausch über das Internet ist allerdings die Existenz der WINSOCK.DLL auf Ihrem System sowie ein Zugang zum Internet über einen Provider.



Sie haben zwei Möglichkeiten der Kommunikation:

1. TCP/IP-Direktverbindung über eine Standleitung

Bei Nutzung der Standleitung ist die Einstellung weiterer Parameter nicht erforderlich.

2. TCP/IP-Wählverbindung über einen Internet-Provider

Bei Anwahl über einen Internet-Provider konfigurieren Sie bitte erst das DFÜ-Netzwerk von Windows und nehmen die notwendigen Einstellungen anhand der Angaben Ihres Providers vor.

<u>DFÜ-Netzwerk:</u>

Wenn Sie Ihren **Zugang über** das **DFÜ-Netzwerk herstellen** können, wählen Sie Ihre **Verbindung** mittels der Auswahlliste aus und tragen **Benutzer** sowie **Passwort** ein. Außerdem können Sie die **Anzahl der Wahlwiederholungen** sowie die **Pause in Sekunden zwischen den Wiederholungen**. Weiterhin können Sie festlegen, ob das System die **Verbindung nach der DFÜ beenden** soll.
Beim Verbindungsaufbau wird zunächst eine Verbindung über das DFÜ-Netzwerk zu Ihrem Provider hergestellt und anschließend die Bank angewählt.

<u>Proxy-Einstellungen:</u>

Wenn Sie einen **Proxyserver verwenden**, markieren Sie das entsprechende Kontrollkästchen. Anschließend können Sie dann die **Adresse** (IP-Adresse in der Form nnn.nnn.nnn.nnn bzw. Hostname, z. B. proxy.xyz.de; keine URL-Angaben) und **Port** des **Proxy**servers sowie einen **Benutzernamen** und **Passwort** dafür eingeben.



☞ **Bitte beachten Sie ...**

Bei EBICS wird der Standard-Port für SSL/TLS-Verbindungen (443) verwendet. Bei anderen Verfahren (z. B. MCFT) legen die Banken spezielle Ports für die Verbindungsaufnahme fest. Falls in Ihrem Proxy die ausgehenden Ports beschränkt sind, müssen dort diese Ports ggf. zusätzlich freigegeben werden. Sie finden die Port-Angaben in der BPD-Datei der jeweiligen Bank bzw. in dem Schreiben mit den Zugangsdaten.

Da die Kommunikation zu den Banken meist automatisch abläuft, müssen die Zugangsdaten in den Proxy-Parametern abgespeichert werden, so dass sie den Kommunikationsprozessen immer zur Verfügung stehen. Wenn Ihr Proxy eine Authentifizierung erwartet, empfehlen wir eine spezielle Kennung für die Electronic Banking-Kommunikation anzulegen, deren Passwort möglichst auch zeitlich unbeschränkt ist. Dies ist kein Sicherheitsrisiko, da die Zugangsdaten verschlüsselt abgespeichert werden.

Die Proxy-Einstellungen werden getrennt je Rechner im Netzwerk verwaltet und verschlüsselt gespeichert. Dadurch kann hier für jeden Rechner (oder seinen Benutzer) eine individuelle Benutzerkennung mit zugehörigem Proxy-Passwort abgelegt werden, so dass dies nicht für jeden Kommunikationsauftrag neu eingegeben werden muss. Dadurch ist auch ein unbedienter Kommunikationsbetrieb möglich.

Um den Betrieb des Electronic-Banking-Systems zu vereinfachen, kann es auch sinnvoll sein, hierfür einen speziellen Proxy-Benutzer anzulegen, dessen Passwort nicht abläuft.

Es werden folgende Proxy-Authentifizierungsverfahren unterstützt:

1. Basic

2. Digest

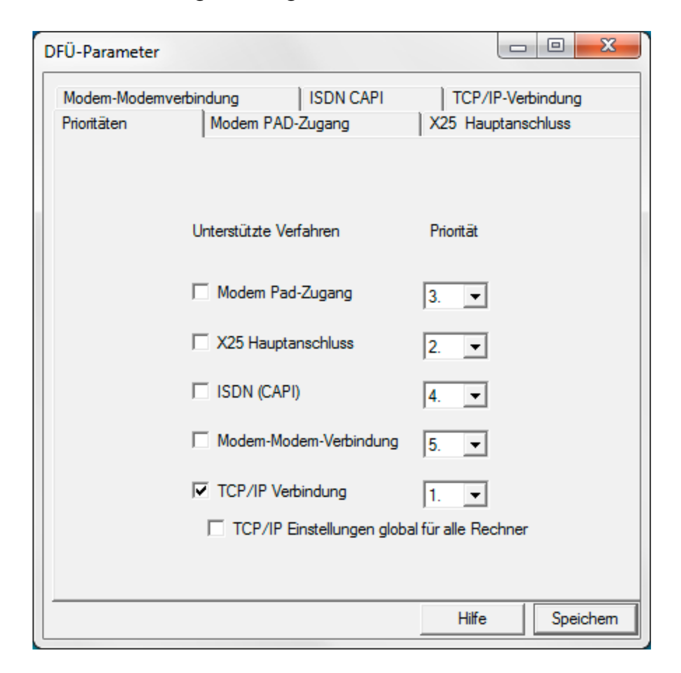
3. NTLM (Microsoft® ISA-Server)

Es sind keine speziellen Einstellungen hierfür vorzunehmen, da die DFÜ-Module beim Verbindungsaufbau mit dem Proxy automatisch das favorisierte Verfahren aushandeln.



2.7 Registerkarte Prioritäten (DFÜ-Verfahren)

Auf der *Registerkarte Prioritäten* bestimmen Sie, in welcher Reihenfolge (Priorität) die zuvor von Ihnen konfigurierten DFÜ-Verfahren vom Programm genutzt werden sollen.



Bei TCP/IP besteht die Besonderheit, dass hier durch Markieren des Kontrollkästchens "**TCP/IP-Einstellungen global für alle Rechner**" definiert werden kann, dass die TCP/IP-Parameter (s. Kapitel 2.6) global gelten sollen. In diesem Fall muss TCP/IP nur einmalig auf einem beliebigen Rechner aktiviert und die Proxy-Parameter ebenfalls nur einmal eingetragen werden. Sie werden dann von allen Rechnern im Netzwerk verwendet.

Die Konfiguration der Übertragungswege zu Ihren Banken (z. B. über ISDN) ist in den verschiedenen BPDs (Bankparameterdateien) festgehalten. Sollten sich Änderungen beim Zugang zu Ihrer Bank ergeben, erhalten Sie von dort entsprechend Nachricht und nehmen in der betreffenden BPD Korrekturen vor. Was dabei zu beachten ist, erfahren Sie in Kapitel 3: *Bankparameterdateien pflegen*..

Für jedes DFÜ-Verfahren lassen sich über eine Auswahlliste die Prioritäten 1 bis 5 festlegen.

Wenn Sie über einen ISDN-Anschluss verfügen, sollten Sie diesem Kommunikationsweg die 1. oder 2. Priorität einräumen. Besteht auch die Möglichkeit einer Nutzung von X.25, so bietet sich dafür die 2. bzw. 3. Priorität an.

Bei Nutzung verschiedener DFÜ-Verfahren prüft das Programm, welche Banken mit dem von Ihnen mit der höchsten Priorität belegten DFÜ-Verfahren arbeiten. Die in den zur Ausführung anstehenden DADs für diese Banken hinterlegten Aufträge werden zuerst abgearbeitet. Anschließend geht das Programm zum DFÜ-Verfahren mit der nächstniedrigeren Priorität über und arbeitet die Aufträge ab, die mit diesem Verfahren ausgeführt werden sollen.



Die Vorgehensweise lässt sich anhand der folgenden Grafik erläutern:

Sie nutzen mit Prioriät :
Ihre Bank bietet an :

1. TCP/IP
2. ISDN
3. X.25
4. Modem

Bank 1: TCP/IP, ISDN, X.25
Bank 2: ISDN, X.25
Bank 3: X.25, Modem
Bank 4: X.25

In dem Beispiel stellt das Programm zunächst die Verbindung mit der Bank 1 unter Nutzung des Internets (= TCP/IP) her und arbeitet alle anstehenden Aufträge ab.
Anschließend wird über ISDN Verbindung mit Bank 2 aufgenommen und alle anstehenden Aufträge werden abgearbeitet. Da bereits per Internet alle Aufträge zur Bank 1 übertragen wurden, wird diese Bank hier nicht mehr angesprochen, es sei denn, die Übertragung per Internet käme nicht zu Stande.
Im nächsten Arbeitsschritt wird per X.25 Verbindung mit Bank 3 und Bank 4 aufgenommen und die Übertragung der restlichen Aufträge wird gestartet. Die DFÜ-Aufträge mit Priorität 1 (Internet) und 2 (ISDN) sind zu diesem Zeitpunkt bereits durchgeführt, so dass nur im Fehlerfall (Internet und ISDN-Kommunikation sind gescheitert) eine X.25-Kommunikation zu den Banken 1 und 2 erfolgt.

Da die Bank 3, die zusätzlich zu X.25 eine Modem-Modem-Kommunikation anbietet, bereits über die Priorität 3 (= X.25) angesprochen wurde, findet keine Modem-Modem-Kommunikation statt. Es sei denn: Sie setzen die Prioritätenliste um und vergeben für die Modem-Modem-Kommunikation eine höhere Priorität als die im Beispiel angegebene Priorität 4.



2.8 AT-Befehle

Die Ansteuerung der für den Programmbetrieb geeigneten Modems erfolgt unter Einsatz des AT-Befehlssatzes, der zu einem Quasi-Standard geworden ist. Es gibt jedoch bei den am Markt erhältlichen Modems Unterschiede in Art und Umfang des AT-Befehlssatzes. Ferner müssen AT-Befehle bei einigen Modems ausschließlich in Großbuchstaben eingegeben werden.

Ein Modem kann AT-Befehle nur dann interpretieren und verarbeiten, wenn es sich im Kommando-Modus befindet (nach dem Einschalten bzw. vor der Datenübertragung).

Im Transparent-Modus dagegen (während der Übertragung) wird kein Zeichen, das zur Gegenstelle gesendet oder von dieser empfangen wird, interpretiert.

Jede AT-Befehlszeile muss mit den Befehlszeilenpräfix "**AT**" oder "**at**" beginnen. Die Buchstaben "AT" werden auch als "**AT**tention Code" bezeichnet. Dieser Code dient dazu, dem Modem zu signalisieren, dass ein oder mehrere Befehle folgen.

Mehrere Befehle können zu einer Befehlszeile zusammengefasst werden, die mit einem <**CR**>-Zeichen enden muss. Die Befehle werden durch Leerzeichen getrennt.

Die Summe der Zeichen einer Befehlszeile darf **40 Zeichen** nicht überschreiten (einschließlich AT-Präfix, Befehle, Leerzeichen und <CR>).

Beispiel für AT-Standardmodem:

Bei allen AT-Modemtypen sind die nachstehenden Einstellungen konstant.

```
Übertragungsart   300 Baud        :  oder 1200, 2400 / 9600 / usw.
                  Telefonmodem
Baud              300             :  oder 1200, 2400 / 9600 / usw.
Parity            None            :
Bits              8 Bit           :
Port              COM1            :  oder COM2, COM3, ..., COM8
Datex-Kennung     xxxxxxxx        :  Ihre NUI von der Post
Datex-Passwort     xxxxxxxx        :  Ihr Passwort von der Post
Modem Init        AT&C1&D2!~~~~   :
Datex-Anwahl      ATDP            :
Nummer            xxxxxxxx        :  Tel.Nr. Datex-Knoten
AT-Standard       [x]             :  "Ankreuzen"
```

Initialisierungstext

Der Text im Feld "Initialisierungstext" sollte bei den meisten AT-Modems die folgenden Einträge enthalten:

```
AT&C1&D2V1!~~~~
     I   I
     I   DTR zeigt an, ob noch Verbindung besteht
    DCD zeigt Carrier an
```

Sollten Sie beim Anwählen die Fehlermeldung "No Dialtone" bekommen, erweitern Sie den Eintrag auf:

AT&C1&D2V1!~~~~ATX1!~~~~



Wählbefehl

Aufbau des Wählbefehls: **ATDabb**

Die einzelnen Buchstaben sind wie folgt zu ersetzen:

a = "T" bei Telefonanschlüssen mit Tonwahl
"P" bei Telefonanschlüssen mit Pulswahl

Bei hausinternen Anschlüssen muss hier ggf. eine "Amtsholung" mit "0W" vorgenommen werden, wobei die "0" für die entsprechende Ziffer steht, die diese Funktion auslöst. Das "W" steht für "Warten, bis die Amtsleitung vorhanden ist".

AT-Befehle (Auswahl):

- ATZ
  Reset.
  Entspricht dem Aus- und Einschalten des Modems.

- ATMn
  Lautsprecherkontrolle.
  Dabei kann "n" folgende Werte annehmen :
  0 = immer aus
  1 = an bei Wahl und Verbindungsaufbau
  2 = immer an
  3 = an bei Warten auf Antwortton

- ATLn
  Lautsprecherstärke.
  Dabei kann "n" folgende Werte annehmen:
  0 = aus
  1 = leise
  2 = laut
  3 = sehr laut

- ATSO=O
  Automatische Rufbeantwortung aus

- ATE
  Befehlsecho aus

- ATD
  Wählen einer Rufnummer

  Wählsonderzeichen:
  T = Tonwahl
  P = Pulswahl
  > = Amtsholung durch Erdtastendruck
  W = Warte auf Amtszeichen
  , = 1 Sekunde Pause vor Bearbeitung des nächsten Wählzeichens (maximal 3 "," hintereinander)

  Beispiel: ATDT0W06920251
  Tonwahl, 0 für Amt, W warten, Amtston, Telefonnummer, Post-PAD

  Beispiel: ATDP0W06920251
  Pulswahl, 0 für Amt, W warten, Amtston, Telefonnummer, Post-PAD

- ATQn
  Rückmeldung.



Wobei "n" folgende Werte annehmen kann:

0 = Rückmeldung an
1 = Rückmeldung aus

- ATVn
  Art der Rückmeldung.
  Wobei "n" folgende Werte annehmen kann:

  0 = Rückmeldung als Ziffer
  1 = Rückmeldung als Wort

- ATX1
  Meldung bei Verbindung CONNECT 1200 bzw. 2400.

- ATX3
  Bewirkt, dass das Modem vor dem Wählen nicht auf ein Freizeichen wartet. Dies ist vor allem bei Nebenstellenanlagen von Bedeutung.

- AT&C1
  gemäß V22bis bzw. V25bis; DCD gibt den Status des Data Carrier der Gegenstation an. Ein ON-Status des DCD zeigt die gültige Verbindung an.

- AT&D2
  Wird das DTR-Signal vom PC auf OFF gesetzt, löst das Modem die Verbindung auf und geht in den Kommando-Modus.

- AT&Sn
  Data-Set-Ready-Signal.
  Dabei kann "n" folgende Werte annehmen:

  0 = Data-Set-Ready-Signal bleibt immer an.
  1 = Data-Set-Ready-Signal ist AUS im Kommando- und im Textmodus.

- AT&W
  Schreibt die aktuelle Einstellungen in den Modemspeicher, so dass sie beim nächsten Einschalten oder ATZ-Befehl wieder aktiv sind.



Inhaltsverzeichnis: Kapitel 3

Seite



3 Bankparameterdateien pflegen

Die Abkürzung **BPD** steht für "**B**ank**p**arameter**d**atei".

In einer Bankparameterdatei werden Schlüsseldaten für den Zugang zu jeweils einer Bank hinterlegt. BPDs sind zur Einrichtung oder Sperrung der Übertragungswege sowie zur Durchführung von DFÜ-Aufträgen erforderlich.

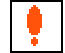
Sie benötigen für **jede** Bank, mit der Sie kommunizieren wollen, eine eigene BPD.

Wenn Sie

- mit dem standardmäßig implementierten DFÜ-Verfahren **ZVDFÜ** arbeiten, erhalten Sie von Ihrer Bank eine Bankdiskette mit den notwendigen Zugangsdaten in Form einer BPD. Die Bezeichnung der Datei besteht in der Regel aus dem Kurznamen der Bank und der Extension ".BPD" (Dateiname in Klammern dahinter).
  Diese Datei können Sie über den mittels der Schaltfläche [***ZVDFÜ-BPD kopieren***] zu öffnenden Auswahldialog aus jedem beliebigen Verzeichnis in das Programm übernehmen (kopieren).

- das erweiterte ZVDFÜ-Verfahren mit Elektronischer Unterschrift (**MCFT**) nutzen, haben Sie u. U. von Ihrer Bank für jeden unterschriftsberechtigten Mitarbeiter eine Diskette mit einer BPD erhalten, die Sie über den mittels der Schaltfläche [***MCFT-BPD importieren***] zu öffnenden Auswahldialog aus jedem beliebigen Verzeichnis in das Programm übernehmen (importieren). Dabei wird eine "**Multi-User-BPD** " angelegt, die für jeden unterschriftsberechtigten Teilnehmer einen Eintrag enthält.

  Aus dem MCFT-Bankparameterdateidialog können einzelne Teilnehmereinträge über die Schaltfläche [***Bankparameterdatei exportieren***]- aus einer Multi-User-BPD entfernt und über den Auswahldialog in jedes beliebige Verzeichnis als einzelne BPD gespeichert (exportiert) werden.

 ZVDFÜ- und MCFT-BPD's **können** nur bezüglich der zu nutzenden Bankparameter, der NUA bzw. des externen und internen Benutzers editiert, **nicht** aber **neu erstellt werden**.

Für alle anderen DFÜ-Verfahren müssen Sie BPDs manuell erstellen. Die dazu erforderlichen Angaben erhalten Sie von Ihrer Bank.

In der aktuellen Programmversion können BPDs erstellt werden für:

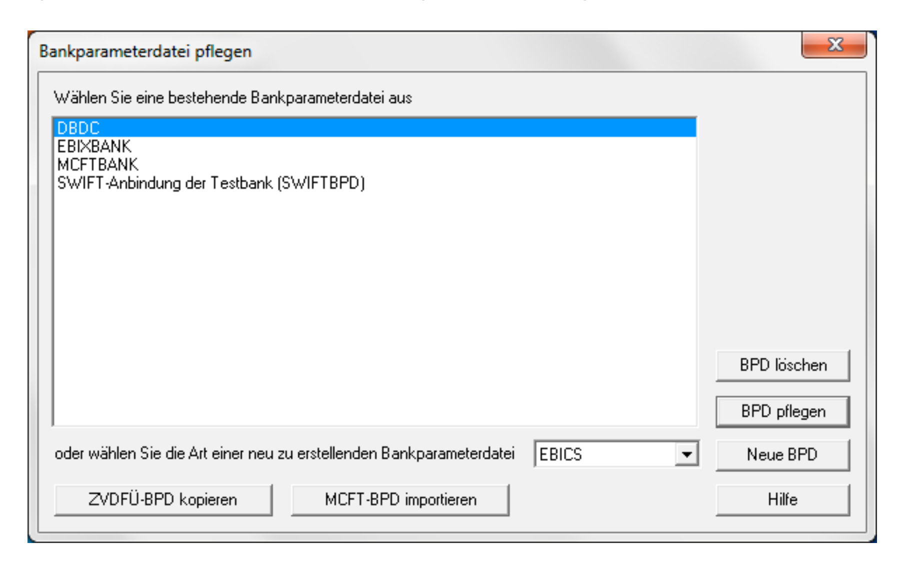
- FTAM
- FTP
- EBICS
- HBCI
- HBCI+
- ETEBAC3
- WOP

Das Verfahren für die Erstellung von BPDs ist bei den oben aufgeführten DFÜ-Verfahren identisch. Unterschiede ergeben sich nur in Art und Umfang der einzutragenden Parameter.



3.1 Erstellen einer BPD

Das Verfahren für die Erstellung von BPDs ist bei den unterstützten DFÜ-Verfahren identisch. Unterschiede ergeben sich nur in Art und Umfang der einzutragenden Parameter.



Folgende Arbeitsschritte sind bei Erstellung einer BPD durchzuführen:

1 **Anwahl des Menüpunktes -Kommunikation- / -Bankparameterdateien-**
Sollte sich im Diskettenlaufwerk für die EU keine Diskette mit einer BPD befinden, werden Sie vom Programm aufgefordert, die Diskette mit der BPD-Datei einzulegen. Mit Drücken der Schaltfläche [***Ja***] ermöglichen Sie nach Einlegen der Diskette den anschließenden Zugriff darauf. Mit [***Nein***] umgehen Sie diese Möglichkeit und es werden alle auf der Festplatte im Unterverzeichnis ..\MCCWIN\DAT vorhandenen BPD-Dateien auflistet. Sie können diesen Arbeitsschritt aber auch über [***Abbrechen***] beenden.
Dateien in Laufwerken sind durch einen Laufwerksbuchstaben in Klammern hinter der Dateibezeichnung gekennzeichnet.

2 **Auswahl der zu erstellenden/editierenden BPD**
Nach Aufruf des Menüpunktes öffnet sich ein Dialog, der die bereits bestehenden Bankparameterdateien anzeigt bzw. über ein Auswahlfeld mit allen unterstüzten DFÜ-Verfahren die Auswahl einer neu zu erstellenden BPD ermöglicht. Wenn Sie

- zu einem bestimmten DFÜ-Verfahren eine BPD **neu anlegen** wollen, wählen Sie die Art der neu zu erstellenden BPD über das Auswahlfeld und drücken anschließend die Schaltfläche [***Neue BPD***].
  In einem Auswahlfenster werden alle bereits im Unterverzeichnis ..\DAT bzw. vorhandenen BPDs angezeigt. Geben Sie den Dateinamen der neu zu erstellenden Datei ein.

  ☞ **Bitte beachten Sie ...**
  Der interne BPD-Dateiname darf maximal 8 Stellen haben und nur aus den Zeichen (A-Z,a-z,0-9,-,_) bestehen.

  Die Extension ".BPD" wird vom Programm automatisch angefügt und der entsprechende Editierdialog wird geöffnet.

- eine bereits vorhandene BPD ansehen und/oder editieren wollen, setzen Sie den Cursor durch Mausklick oder mittels der Richtungstasten auf die gewünschte bestehende BPD und betätigen Sie die Schaltfläche [***Datei pflegen***].
  Doppelklick auf den Eintrag in der Liste öffnet den Editierdialog ebenso.



3 **Eingabe der BPD-Bezeichnung / der Parameter**
In Abhängigkeit von dem in der ausgewählten BPD hinterlegten DFÜ-Verfahren werden unterschiedliche Dialogboxen zur Aufnahme der Parameter angezeigt. Geben sie zunächst eine **Bezeichnung der Bankparameterdatei** ein, die bis zu 30 Zeichen lang sein kann.

Informationen zur Eingabe der Parameter finden Sie unter

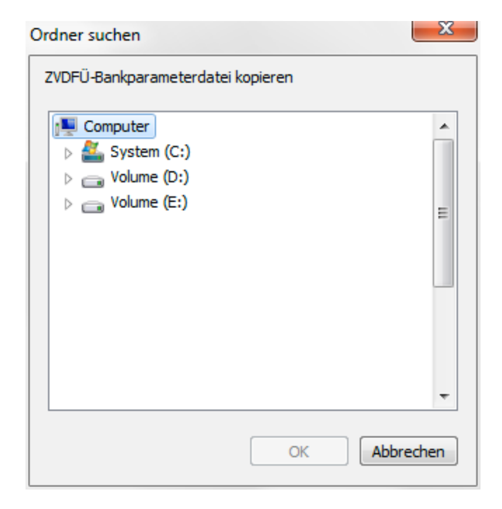
- ZVDFÜ / MCFT
- FTAM
- FTP
- EBICS
- HBCI
- HBCI+
- ETEBAC3
- WOP

4 **Abspeichern der Eingaben mit** [***Speichern***].
Durch Bestätigung über die Schaltfläche [***Speichern***] werden die Einstellungen in die jeweilige Bankparameterdatei übernommen.

 **Beachten Sie bitte ...**
ZVDFÜ- und MCFT-BPDs **können** nur bezüglich der zu nutzenden Bankparameter, der NUA bzw. des externen und internen Benutzers editiert, **nicht** aber **neu erstellt werden**.

Übrigens:
ZVDFÜ-BPDs **können** Sie über die Schaltfläche [***ZVDFÜ-BPD kopieren***] von Diskette in das Festplattenverzeichnis ..\MCCWIN\DAT übernehmen, d. h. auch, ZVDFÜ-BPDs können auf der Diskette verbleiben.

Möchten Sie jedoch die ZVDFÜ-BPD von der Diskette auf die Festplatte übertragen, werden Sie nach Drücken der Schaltfläche [***ZVDFÜ-BPD kopieren***] aufgefordert, die Diskette mit Ihrer ZVDFÜ-BPD in das Diskettenlaufwerk für die EU einzulegen.

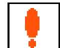


Nach dem Einlegen und Bestätigen über [***OK***] werden in einem Auswahlfenster die auf Diskette vorhandenen BPDs aufgelistet. Durch Cursorpositionierung und Bestätigen mit [***OK***] bzw. durch Doppelklick mit der Maus wählen Sie die zu kopierende BPD aus.





Sollte die BPD bereits auf der Festplatte vorhanden sein, werden Sie gefragt, ob Sie die BPD auf der Festplatte durch die neue BPD ersetzen möchten. Wenn ja, bestätigen Sie mit [***OK***]. Andernfalls brechen Sie den Vorgang hier über [***Abbrechen***] ab.



Bietet Ihre Bank eine Kommunikation per MCFT an, so erhalten Sie von der Bank für jeden zur Durchführung von DFÜ-Aufträgen autorisierten Mitarbeiter eine vollständig konfigurierte Bankparameterdatei auf Diskette. Diese **MCFT**-BPD's **müssen** importiert werden. Benutzen Sie dazu die Schaltfläche [***MCFT-BPD importieren***]. Nähere Informationen finden Sie in Kapitel 3.2.1: *MCFT-BPD importieren*.

Sie können Bankparameterdateien auch wieder löschen, indem Sie die entsprechende BPD auswählen, anschließend die Schaltfläche [***BPD löschen***] betätigen und die folgende Sicherheitsabfrage mit [***Ja***] beantworten.



3.2 ZVDFÜ / MCFT

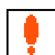
Die Abkürzung **ZVDFÜ** steht für **Z**ahlungs**v**erkehrs-**D**aten**f**ern**ü**bertragung und kennzeichnet das standardmäßig mit dem Basismodul installierte DFÜ-Verfahren. ZVDFÜ beinhaltet:

- Prüfung auf fehlerfreie Datenfernübertragung
- Komprimierung
- Verschlüsselung
- Syntaktische Prüfung (Validierung) der zu übertragenden Daten
- Autorisierung während der Übertragung
- Gewährleistung eines Manipulationsschutzes.

Ein Datenaustausch mit ZVDFÜ kann über die Kommunikationsnetze X.25 (Datex-P), ISDN und das Telefonnetz durchgeführt werden. Jede Bank, mit der Sie eine Vereinbarung zur Teilnahme am Electronic-Banking-Verfahren getroffen haben, stellt Ihnen bei Einsatz von ZVDFÜ eine BPD zur Verfügung. Die Bezeichnung dieser BPD besteht in der Regel aus dem Kurznamen der Bank und der Extension ".BPD".

Sollten sich einmal Änderungen in den von einer Bank angebotenen DFÜ-Verfahren (z. B. Änderung einer NUA) ergeben, so kann die BPD von Ihnen den geänderten Bedingungen angepasst werden. Welche Eintragung wie zu ändern ist, wird Ihnen in solchen Fällen von der Bank mitgeteilt.

Das erweiterte ZVDFÜ-Verfahren mit Elektronischer Unterschrift nennt sich **MCFT** (= **M**ulti**C**ash-**F**ile **T**ransfer). Es beinhaltet die gesamte Funktionalität des ZVDFÜ-Verfahrens, unterstützt jedoch zusätzlich für die Autorisierung von Zahlungsaufträgen die in Kapitel 6 beschriebene Elektronische Unterschrift. Im Gegensatz zum Kommunikationsverfahren FTAM findet hier die Unterschriftsprüfung jedoch während der Datenfernübertragung statt, so dass Sie direkt nach Übertragung der Nutzdaten anhand der Antwort-Codes (vgl. Kapitel 5.4: *Antwort-Codes*) das Ergebnis des DFÜ-Auftrages inklusive der Unterschriftsprüfung erhalten.



Bitte nehmen Sie auf keinen Fall selbständig und ohne Aufforderung durch die Bank Änderungen in den BPDs vor. Es besteht die Möglichkeit, dass Sie durch willkürliche Änderungen Ihren eigenen Zugang zur Bank sperren. Eine Ausnahme bilden die weiter unten beschriebenen Felder mit den "internen" und "externen Namen" der Teilnehmer des MCFT-Verfahrens.

Die Eingabemaske zu einer ZVDFÜ-BPD enthält die Zeilen:

- Bezeichnung der Bankparameterdatei
- Teilnehmernummer
- Kundennummer
- Bankparameter
- X.25 NUA
- ISDN-Rufnummer
- Modemnummer
- TCP/IP IP-Adresse und Port
- Verbindungsinformationen zum Zugang über DFÜ-Netzwerk

Die einzelnen Felder haben die folgende Bedeutung:

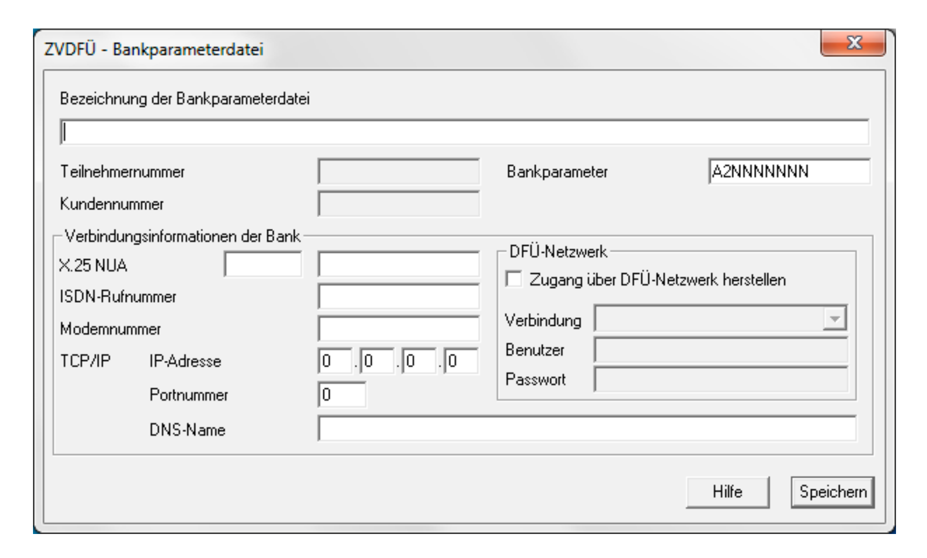
Bezeichnung der Bankparameterdatei

In dieses Feld tragen Sie eine aussagekräftige Bezeichnung der BPD ein, die im weiteren Programmverlauf immer anstelle des Dateinamens der BPD verwendet wird.



Teilnehmernummer
Kundennummer

Die Einträge in den Feldern "Teilnehmernummer" und "Kundennummer" werden bankseitig festgelegt und können daher nicht von Ihnen geändert werden.

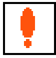


Verbindungsinformationen der Bank:

X.25 NUA
ISDN-Rufnummer
Modemnummer

Die Rufnummern für eine X.25- (Datex-P-), ISDN- und/oder Modem-Kommunikation müssen jeweils nur dann gefüllt werden, wenn die korrespondierenden Felder der Bankparameter gesetzt (= "J") sind. Konkret sind dies die Felder 6 (Datex-P = "J" oder "N"), 7 (ISDN = "J" oder "N") und 8 (Modem = "J" oder "N"). Ist das korrespondierende Feld in der Bankparameterzeile ausgeschaltet (= "N"), so ist es nicht erforderlich, die entsprechende Rufnummer einzutragen.

Das Programm nimmt unter Nutzung des entsprechenden DFÜ-Verfahrens mit Hilfe der Rufnummer aus der BPD Kontakt mit Ihrer Bank auf. Die Rufnummer(n) werden Ihnen von der Bank mitgeteilt.
Bei X.25 (Datex-P) haben Sie die Möglichkeit, in dem vorderen der beiden Felder eine Vorwahlnummer anzugeben.

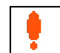


Bitte nehmen Sie **nur auf Anweisung Ihrer Bank** Änderungen an den Rufnummern vor.

TCP/IP

Verfügt Ihr Kreditinstitut über einen Internet-Zugang, so können Sie beliebige Sende- (z. B. Zahlungsaufträge) und Abholaufträge (z.B. Kontoinformationen) über das Internet abwickeln. In diesem Fall sind die Felder "TCP/IP **IP-Adresse**" und "TCP/IP **Portnummer**" bei Erhalt Ihrer BPD bereits gefüllt. Die Adressierung kann anstatt über die IP-Adresse auch mittels **DNS-Name** erfolgen. Dies erleichtert die Änderung der Adresse bei Umzug oder Providerwechsel.

Voraussetzung für den Datenaustausch über das Internet ist allerdings die Existenz der WINSOCK.DLL auf Ihrem System sowie ein Zugang zum Internet über einen Provider (z. B. T-Online, AOL oder Compuserve).



Bitte nehmen Sie **nur auf Anweisung Ihrer Bank** Änderungen an der IP-Adresse, der Portnummer oder dem DNS-Namen vor.



DFÜ-Netzwerk:

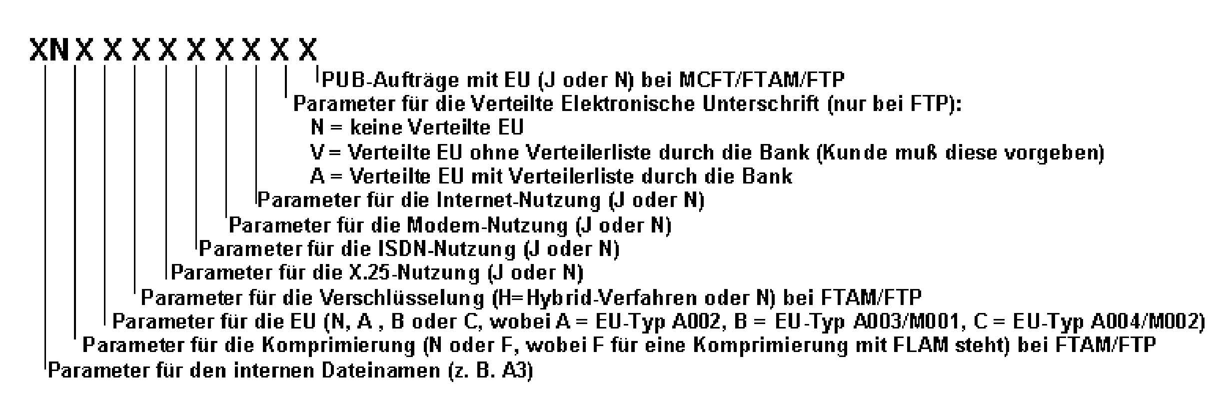
Wenn Sie Ihren **Zugang über** das **DFÜ-Netzwerk herstellen** möchten, konfigurieren Sie bitte zuvor das DFÜ-Netzwerk von Windows und nehmen die notwendigen Einstellungen anhand der Angaben Ihres Internet-Providers vor. Wählen Sie Ihre **Verbindung** mittels der Auswahlliste aus und tragen **Benutzer** sowie **Passwort** ein.

Bankparameter

Das Feld "Bankparameter" ist eine Zeichenkette bestehend aus einer Kombination von Buchstaben und Ziffern.

Bitte beachten Sie, dass das Bankparameterfeld die bankseitig unterstützten Parameter beschreibt, d. h. kundenseitig kann z. B. die Kommunikation via ISDN zu einer bestimmten Bank nur dann genutzt werden, wenn im entsprechenden Feld der Bankparameter-Zeichenkette ein "J" eingetragen wurde.

Die einzelnen Felder der Bankparameter haben die folgende Bedeutung:



Eine typische **ZVDFÜ**-Bankparameterzeile ist z. B. wie folgt aufgebaut: **A3NNNJJNNNN**

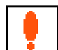
- der interne Dateiname wird mit **A3** beginnend gebildet
- es ist keine gesonderte Komprimierung und keine gesonderte Verschlüsselung erforderlich, da diese Funktionalitäten bereits im ZVDFÜ-Verfahren integriert sind, eine Elektronische Unterschrift ist nicht vorgesehen
- zur Kommunikation mit der Bank kann wahlweise X.25 (Datex-P) oder ISDN genutzt werden
- Modem- und Internet-Kommunikation wird bankseitig nicht unterstützt
- eine Verteilte Elektronische Unterschrift wird bankseitig nicht unterstützt
- die Erteilung von PUB-Aufträgen mit Elektronischer Unterschrift ist nicht vorgesehen

Eine typische **MCFT**-Bankparameterzeile ist z. B. wie folgt aufgebaut: **A3NBNJJNJNJ**

- der interne Dateiname wird mit **A3** beginnend gebildet
- es ist keine gesonderte Komprimierung erforderlich, da diese bereits im MCFT-Verfahren integriert ist
- die zu übertragenden Dateien werden mit einer Elektronischen Unterschrift der Version M001 abgesichert
- es wird keine gesonderte Verschlüsselung benötigt, da diese bereits im MCFT-Verfahren integriert ist
- zur Kommunikation mit der Bank kann wahlweise X.25 (Datex-P) oder ISDN genutzt werden
- eine Modem-Kommunikation wird bankseitig nicht unterstützt
- ein Datenaustausch via Internet wird bankseitig unterstützt
- eine Verteilte Elektronische Unterschrift wird bankseitig nicht unterstützt
- die Erteilung von PUB-Aufträgen mit Elektronischer Unterschrift ist möglich



Änderungen sind in der Regel nur an den vier Feldern für die DFÜ-Zugänge (X.25/Datex-P, ISDN, Modem und Internet) vorzunehmen.



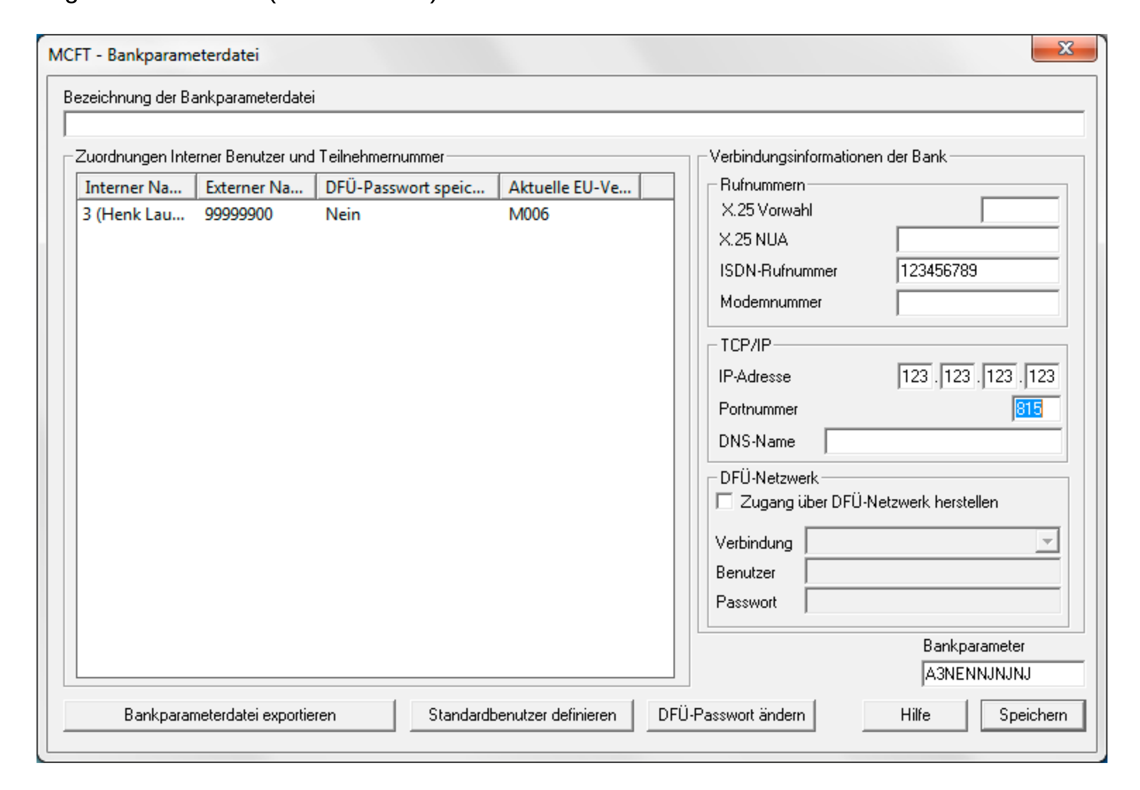
Bitte nehmen Sie **nur auf Anweisung Ihrer Bank** Änderungen an diesen Parametern vor.

Zuordnungen Interner Benutzer und Teilnehmernummer bei der Bank:

Teilnehmernummer (externer Name)

Bei **MCFT** sind die BPDs um die Tabelle der "internen" und "externen Namen" ergänzt. Die Tabelle dient der Zuordnung der internen Namen (Benutzernamen) zu den Teilnehmernummern bei der Bank. Bis zu 512 Unterschriftsberechtigte können in einer BPD gespeichert werden.

Die bankseitig definierten **Teilnehmernummern** (externen Namen) erhalten Sie von Ihrer Bank (mit der BPD). Jeder Kunden-ID können mehrere Teilnehmernummern zugeordnet werden.
Die Teilnehmernummern können von Ihnen über eine Auswahlliste den im System angemeldeten Benutzern zugeteilt werden. Dabei prüft das Programm, ob die über den Menüpunkt -Benutzer- / -Benutzer pflegen- definierten **Benutzernamen** mit den Einträgen unter **"Interner Name"** identisch sind.
Nur die unter "Interner Name" eingetragenen Benutzer, denen eine Teilnehmernummer zugeteilt wurde, können Daten via MCFT mit einer Bank austauschen.
Durch zweimaliges Anklicken mit der linken Maustaste in der Auflistung bzw. über den Kontextmenüeintrag -Datensatz pflegen- (rechte Maustaste) öffnet sich die Liste der verfügbaren Benutzer (interer Name).



Bankparameterdatei exportieren

Über die Schaltfläche [***Bankparameterdatei exportieren***] (s. Kapitel 3.2.2: *MCFT-BPD exportieren*) können einzelne Teilnehmereinträge aus einer "Multi-User-BPD" (s. Kapitel 3.2.1: *MCFT-BPD importieren*) entfernt und wieder als einzelne BPD gespeichert werden.

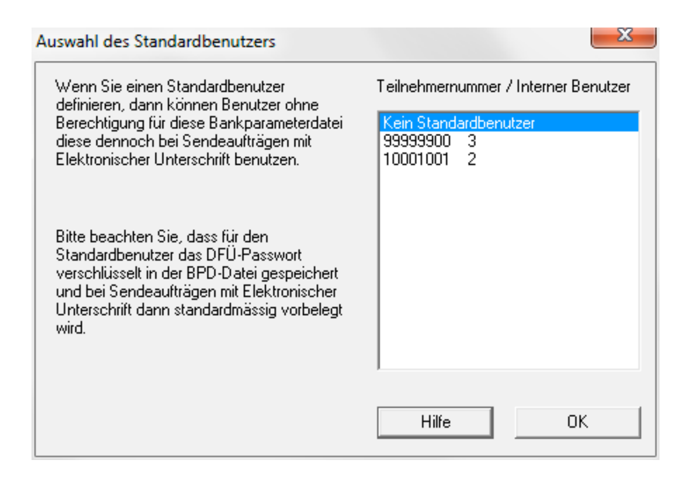


Standardbenutzer definieren

Über die Schaltfläche [***Standardbenutzer defininieren***] können Sie einen sogenannten Standardbenutzer definieren. Benutzer ohne Berechtigung für diese MCFT-Bankparameterdatei können diese dann dennoch für Sendeaufträge mit Elektronischer Unterschrift nutzen.

 **Bitte beachten Sie:**

Nach der Definition eines Standardbenutzers muss erst eine Verwaltungsauftragsart wie INI oder PWA mit dem Standardbenutzer durchgeführt werden. Das DFÜ-Passwort für den Standardbenutzer wird dann verschlüsselt in der Bankparameterdatei gespeichert und bei Sendeaufträgen mit Elektronischer Unterschrift standardmäßig vorbelegt.



DFÜ-Passwort ändern

Über die Schaltfläche [***DFÜ-Passwort ändern***] können Sie das Passwort, das in der BPD abgespeichert ist, ändern. (Das Passwort, das der Bank bekannt ist, wird hiermit nicht geändert! Dazu muss die Auftragsart PWA ausgeführt werden bzw. über -Kommunikation- / -DFÜ-Passwort ändern- [Assistent] das Passwort beim Bankrechner geändert werden.)
Jeder Benutzer aus der Bankparameterdatei kann dazu ausgewählt werden. Sie geben einfach das neue Passwort ein. Da die Passworteingabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit wiederholen. Sie bestätigen anschließend Ihre Eingaben mit <**Return**> oder durch Anklicken von [***Speichern***].



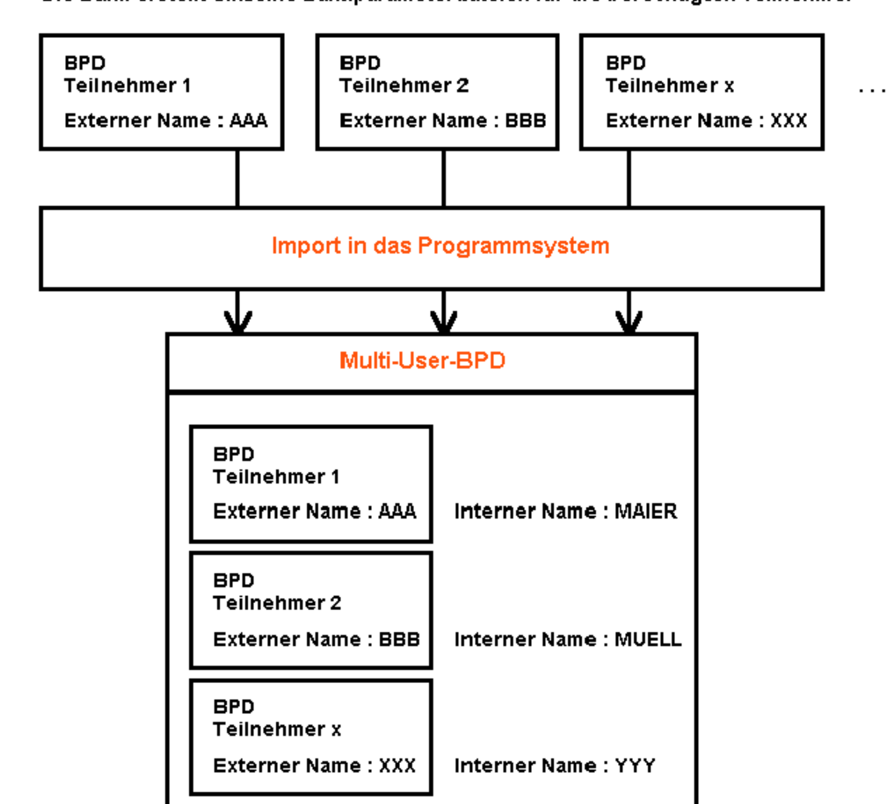


3.2.1 MCFT-BPD importieren

Bietet Ihre Bank eine Kommunikation per **MCFT** (vgl. Kapitel 1.2.2: *MCFT*) an, so erhalten Sie von der Bank für jeden zur Durchführung von DFÜ-Aufträgen autorisierten Mitarbeiter eine vollständig konfigurierte Bankparameterdatei auf Diskette. Die auf den einzelnen Disketten enthaltenen Bankparameterdateien können Sie zur einer "**Multi-User-BPD**" zusammenfassen. Selbstverständlich können Sie die BPDs auch einzeln nutzen.

Unter dem Begriff "**Multi-User-BPD**" ist folgendes zu verstehen:
Durch entsprechende Zuordnung ist auf Bankseite festgelegt worden, dass auf ein Konto mehrere Benutzer (= Teilnehmer) sowohl bei Sende- als auch bei Abholaufträgen zugreifen können. Für diese Benutzer wurde ein "externer Name" (=Teilnehmernummer) im Banksystem abgespeichert. Alle Benutzer, für die die BPD einen "externen Namen" enthält, können mit dieser BPD arbeiten. Es braucht also nicht für jeden Benutzer eine eigene BPD vorhanden zu sein.

Der Zusammenhang lässt sich anhand der folgenden Grafik erläutern:



Über die Schaltfläche [***MCFT-BPD importieren***] können Sie vor der Pflege der BPD-Datei (s. Kapitel 3.1 *Erstellen einer BPD*) aus der Vielzahl der Einzel-BPDs für einen Bankzugang eine einzige "Multi-User-BPD" generieren. Diese "Multi-User-BPD" kann nur auf der Festplatte gehalten werden; eine "Auslagerung" auf Diskette ist nicht möglich.

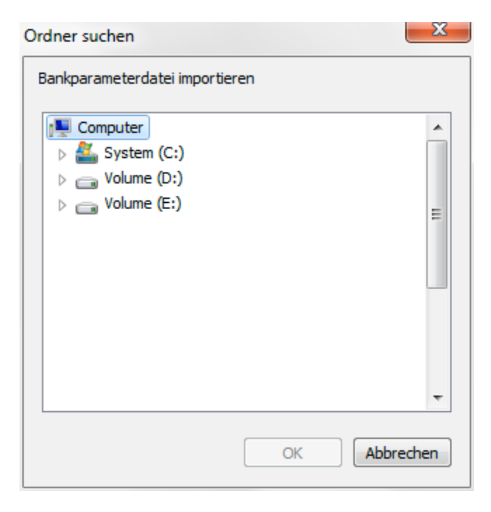
Die "Multi-User-BPD" bietet den Vorteil, dass bei der Durchführung von DFÜ-Aufträgen mit **einer** Bank **alle Benutzer** immer nur auf **eine einzige BPD** zugreifen. Dieser BPD kann eine eindeutige Bezeichnung zur Identifikation der betreffenden Bank zugewiesen werden.



Folgende Arbeitsschritte sind zum **Import einer MCFT-BPD** bzw. zum Erstellen einer "Multi-User-BPD" notwendig:

1 Auswählen der Schaltfläche [***MCFT-BPD importieren***].

2 Auswahl des Verzeichnisses, wo sich die Bankparameterdatei befindet.



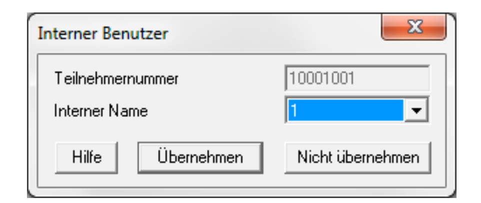
3 Auswahl der MCFT-BPD aus einer Übersicht der im gewählten Verzeichnis befindlichen BPD-Dateien, von der Teilnehmerdaten übernommen werden sollen. Markieren Sie die gewünschte BPD durch Cursorpositionierung bzw. Anklicken mit der Maus und Bestätigen mit [***OK***].



4 Zuordnung der **Teilnehmernummer** ("externer Name") zu einem internen Benutzer. Diesen Benutzernamen (= **interner Name**) desjenigen Anwenders, der u. a. mit der neuen "Multi-User-BPD" arbeiten soll, wählen Sie über eine Auswahlliste, die alle im Kundensystem geführten Benutzer anbietet. Bestätigen Sie Ihre Auswahl durch Drücken der Schaltfläche [***Übernehmen***]. Sind weitere Teilnehmer vorhanden, wiederholt sich der Vorgang solange, bis alle Teilnehmer internen Benutzern zugeordnet wurden. Möchten Sie einen Teilnehmer nicht importieren, drücken Sie die Schaltfläche [***Nicht übernehmen***].

☞ **Beachten Sie bitte:**
Beim "Import" ist das Feld "interner Name" immer mit dem Namen des angemeldeten Benutzers vorbelegt.





Übrigens:

Bei der Erstellung bzw. Erweiterung einer "Multi-User-BPD" werden immer "Paare" aus dem von der Bank vorgegebenen "externen" Namen und einem "internen" Namen gebildet. Es findet also eine Zuordnung eines "internen" Benutzernamens zu einem bankseitigen "externen" Namen statt.

Die in einer "Multi-User-BPD" enthaltenen Paare aus "externen" und "internen" Namen können unter -Kommunikation- jederzeit über den Menüpunkt -BPD-Dateien- angezeigt werden. Genauere Informationen finden Sie in Kapitel 3.1*: Erstellen einer BPD*.



3.2.2 MCFT-BPD exportieren

Die über die Schaltfläche [***MCFT-BPD importieren***] aus mehreren Einzel-BPDs zusammengeführte "**Multi-User-BPD**" kann im Dialog "MCFT-Bankdaten" über die Schaltfläche [***Bankparameterdatei auf Diskette exportieren***] wieder in Einzel-BPD´s aufgeteilt werden. Die Einzel-BPD wird beim "Export" auf eine Diskette abgespeichert.

Ein "Export" kann beispielsweise erforderlich sein, wenn ein in der "Multi-User-BPD" enthaltener Teilnehmer

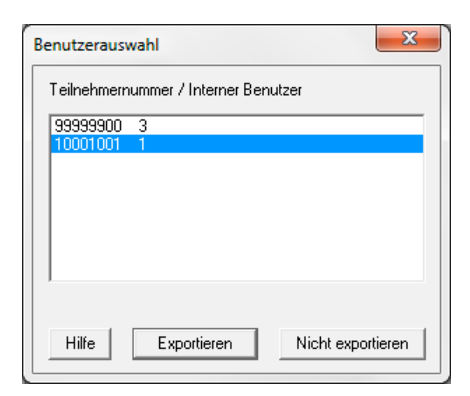
- das Unternehmen verlässt und der für ihn eingerichtete Kommunikationsweg gelöscht werden soll
- in eine andere Abteilung oder eine Zweigstelle des Unternehmens wechselt und dort den für ihn eingerichteten Kommunikationsweg weiterhin nutzen soll.
- etc.

Im ersten Fall sollte die auf Diskette "exportierte" Einzel-BPD gelöscht werden; im zweiten Fall nimmt der Anwender "seine" auf Diskette abgespeicherte Einzel-BPD mit zu seinem neuen Arbeitsplatz und kann sie dort - wie bisher - weiter nutzen.

Folgende Arbeitsschritte sind beim **Exportieren von Einzel-BPDs** aus einer "Multi-User-BPD" durchzuführen:

1 Auswählen der MCFT-"Multi-User-BPD", aus der eine einzelne BPD exportiert werden soll

2 Drücken der Schaltfläche [***Bankparameterdatei exportieren***].



3 Auswählen des Teilnehmers (identifiziert durch Teilnehmernummer und "internen" Benutzernamen), dessen BPD exportiert werden soll. Markieren Sie einen oder mehrere zu exportierende(n) Teilnehmer durch Cursorpositionierung bzw. Anklicken mit der Maus und drücken Sie anschließend die Schaltfläche [***Exportieren***].

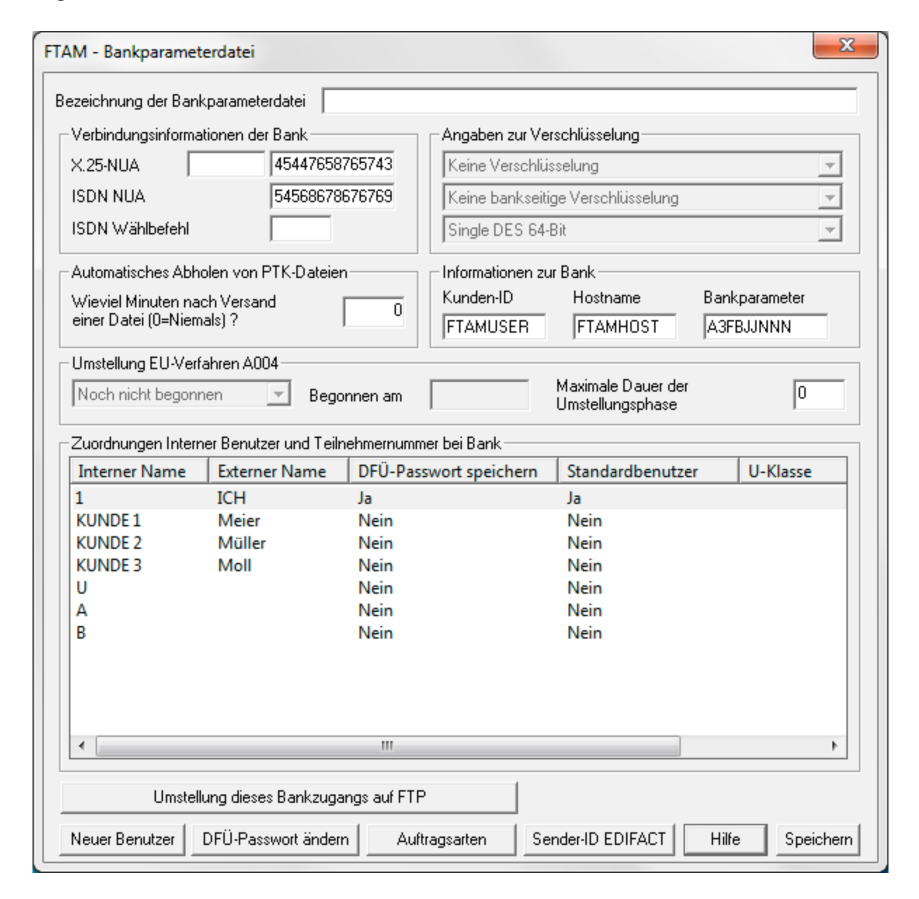
4 Zielverzeichnis für Export aus Verzeichnisstruktur auswählen und mit [***OK***] bestätigen
ggf. Einlegen eines Datenträgers in ein entsprechendes Laufwerk (auf diesen Datenträger wird dann die aus der "Multi-User-BPD" exportierte Einzel-BPD geschrieben).



3.3 FTAM

FTAM (**f**ile **t**ransfer **a**ccess **m**ethod) ist ein standardisiertes Verfahren zur Übertragung beliebiger Dateien. FTAM erlaubt einen Zugriff auf Inhalt und Attribute einer Datei auf einem über ein Netz erreichbaren offenen System.

Bei einer FTAM-Kommunikation müssen Sie **für jede Bank eine gesonderte Bankparameterdatei** erzeugen. Im Gegensatz zu ZVDFÜ/MCFT erhalten Sie bei FTAM keine BPD von Ihrer Bank.



Bei Generierung einer FTAM-BPD stehen Ihnen die folgende Felder zur Verfügung:

Bezeichnung der Bankparameterdatei

In dieses Feld tragen Sie eine aussagekräftige Bezeichnung der BPD ein (max. 30 Zeichen), die im weiteren Programmverlauf anstelle des Dateinamens der BPD verwendet wird.

Verbindungsinformationen der Bank:

Die erforderlichen Angaben zur Konfiguration der Felder werden Ihnen von Ihrer Bank mitgeteilt.

- X.25- Präfix (Länderkennung)
- X.25- NUA
- ISDN NUA
- ISDN Wählbefehl (z. B. für Nebenstellenanlage, Provider-Vorwahl)



Angaben zur Verschlüsselung:

Unter "**Angaben zur Verschlüsselung**" finden Sie Angaben dazu, ob die kundenseitige oder die bankseitige Verschlüsselung über den Menüpunkt -Kommunikation- / -Verschlüsselung- (s. Kapitel 4.5) in Betrieb genommen wurde und welcher Schlüssel für die Verschlüsselung gewählt wurde. Wurde keine Verschlüsselung zwischen Kunde und Bank vereinbart, befinden sich die Statusangaben auf: "Keine kundenseitige bzw. bankseitige Verschlüsselung". Nach Einstellung der Auftragsarten VPK bzw. VPB in die entsprechenden DADs finden Sie hier die Statusangaben "Kundenseitige bzw. bankseitige Verschlüsselung vorbereitet". Nach erfolgreichem Austausch der Schlüssel ändern sich die Angaben auf "Kundenseitige bzw. bankseitige Verschlüsselung aktiviert".

Automatisches Abholen von PTK-Dateien:

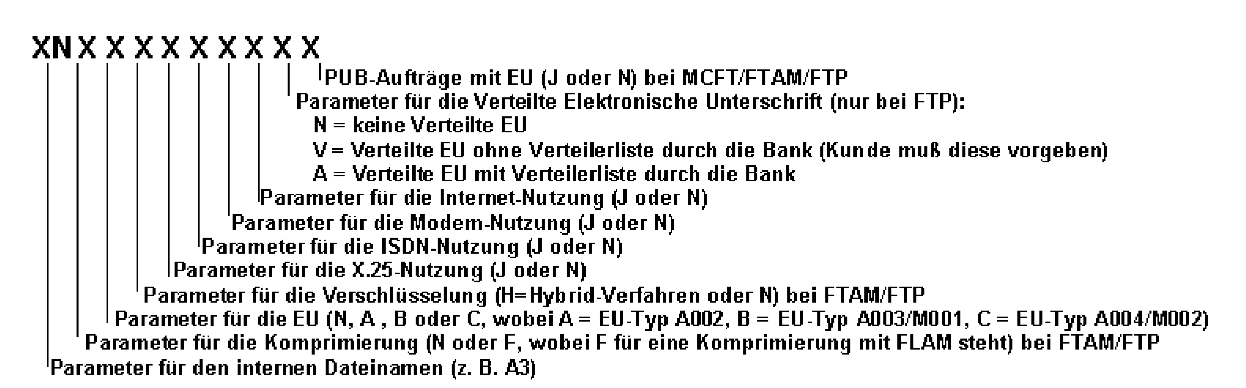
Wenn Sie hier hinter dem Feld: "Wieviel Minuten nach Versand einer Datei?" die Vorbelegung 0 durch eine Zahl ersetzen, erfolgt nach der entsprechenden Zeit **nach** einem FTAM-Sendeauftrag ein automatischen Abholen der zugehörigen Protokollinformationen. Bei "0" erfolgt kein automatisches Abholen.

Informationen zur Bank:

Die bankseitig definierte **Kunden-ID** dient bei allen DFÜ-Aufträgen der Identifizierung des Kunden. Der Bankrechner akzeptiert Ihre DFÜ-Aufträge nur, wenn Sie bei Ihrer Bank über eine Kunden-ID verfügen.
Den **Hostname**n und die **Bankparameter** bekommen Sie ebenfalls von Ihrer Bank mitgeteilt. Das Feld "Bankparameter" enthält eine Zeichenkette bestehend aus einer Kombination von Buchstaben und Ziffern.

Bitte beachten Sie, dass das Bankparameterfeld die bankseitig unterstützten Parameter beschreibt, d. h. kundenseitig kann z. B. die Kommunikation via ISDN zu einer bestimmten Bank nur dann genutzt werden, wenn im entsprechenden Feld der Bankparameter-Zeichenkette ein "J" eingetragen wurde.

Die einzelnen Felder der Bankparameter haben die folgende Bedeutung:

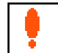


Eine typische **FTAM**-Bankparameterzeile ist z. B. wie folgt aufgebaut: **A3FCHJJNNNJ**

- der interne Dateiname wird mit **A3** beginnend gebildet
- Dateien können mit dem Verfahren FLAM komprimiert werden
- die zu übertragenden Dateien werden mit einer Elektronischen Unterschrift der Version A004 abgesichert
- Verschlüsselung ist möglich (Hybridverfahren)
- zur Kommunikation mit der Bank kann wahlweise X.25 (Datex-P) oder ISDN genutzt werden
- eine Modem-Kommunikation wird bankseitig nicht unterstützt
- ein Datenaustausch via Internet ist nicht möglich
- eine Verteilte Elektronische Unterschrift wird bankseitig nicht unterstützt
- die Erteilung von PUB-Aufträgen mit Elektronischer Unterschrift ist möglich



Änderungen sind in der Regel nur an den vier Feldern für die DFÜ-Zugänge (X.25/Datex-P, ISDN, Modem und Internet) vorzunehmen.



Bitte nehmen Sie **nur auf Anweisung Ihrer Bank** Änderungen an diesen Parametern vor.

Umstellung EU-Verfahren A004:

Unter "**Umstellung EU-Verfahren A004**" erfahren Sie Angaben zum Status der Umstellung des EU-Verfahrens (noch nicht begonnen, kann beginnen, hat begonnen, fertig), zum Beginn der Umstellung ("**Begonnen am**") und zur **maximale**n **Dauer der Umstellungsphase** (standardmäßig 60 Tage). Weitere Informationen dazu finden Sie in Kapitel 6.3: *Unterschriftsversion umstellen*.

Zuordnungen Interner Benutzer und Teilnehmernummer bei der Bank:

Zusätzlich zur Kunden-ID legen Sie interne und externe Namen für die einzelnen Anwender fest, die mit der jeweiligen BPD arbeiten dürfen. Bis zu 512 Unterschriftsberechtigte können in einer BPD gespeichert werden.

Die bankseitig definierten "**externen Namen**" erhalten Sie vom Serviceberater Ihrer Bank. Jeder Kunden-ID können mehrere externe Namen zugeteilt werden.
Die externen Namen können von Ihnen bestimmten Benutzern zugeteilt werden. Unter "**interner Name**" können Sie über ein Listenfeld aus den im Menüpunkt -Benutzer- definierten **Benutzernamen** wählen. Nur die unter "interner Benutzer" eingetragenen Benutzer, denen ein "externer Name" zugeteilt wurde, können Daten via FTAM mit einer Bank austauschen.

Durch zweimaliges Anklicken mit der linken Maustaste in der Auflistung bzw. über den Kontextmenüeintrag -Datensatz pflegen- (rechte Maustaste) öffnet sich die Liste der verfügbaren Benutzer (interer Name). Anschließend kann der externe Namen eingegeben werden. Über den Kontextmenüeintrag -Neuaufnahme Benutzer- bzw. über die Schaltfläche [***Neuer Benutzer***] können neue Benutzer (aus dem am Rechner verfügbaren) in die BPD aufgenommen werden (neuer Datensatz). Über -Löschen- und Bestätigen der Sicherheitsabfrage mit [***Ja***] können Benutzereinträge aus der BPD entfernt werden.

Zusätzlich kann für jeden Benutzer festgelegt werden, ob das DFÜ-Passwort in der Bankparameterdatei gespeichert werden soll. Dazu wählen Sie in der Spalte "**DFÜ-Passwort speichern**" aus der Liste entweder "Ja" oder "Nein".
Das DFÜ-Passwort wird in der Bankparameterdatei vorgehalten und automatisch bei Sendeaufträgen mit Elektronischer Unterschrift in den DFÜ-Auftrag eingestellt. Damit entfällt auch bei der Aktivierung der Verschlüsselung -sofern diese durch Elektronische Unterschrift legitimiert wird- die manuelle Eingabe des DFÜ-Passwortes je Bank.

Analog zu MCFT kann ein Benutzer als Standardbenutzer definiert werden. Dazu wählen Sie in der Spalte "**Standardbenutzer**" aus der Liste entweder "Ja" oder "Nein".

Nach Ausführen der Auftragsart BPD "Bankparameter-Datei abholen" wird in das Feld "**U**(nterschrifts)**-Klasse** diejenige Unterschriftsklasse eingetragen, die auf Bankseite für Sie definiert wurde:

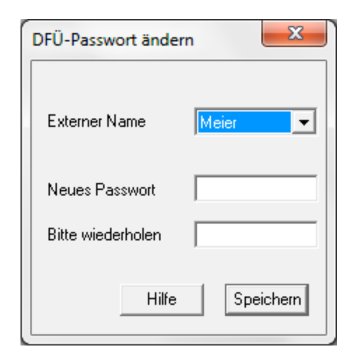
N	keine Unterschrift erforderlich
E	Berechtigung zur Einzelunterschrift bis zum Höchstbetrag
A	Berechtigung zur Erstunterschrift mit beliebiger EU-Berechtigung bis zum Höchstbetrag
B	Berechtigung nur zur Zweitunterschrift bis zum Höchstbetrag

Im Zuge der Erhöhung des Signierschlüssels der EU auf eine Länge von 1024 Bit wurde der Bereich der Zuordnungen um eine Spalte mit der vom jeweiligen Teilnehmer verwendeten EU-Version erweitert (A003 oder A004). Unter "Umstellung EU-Verfahren A004" erfahren Sie

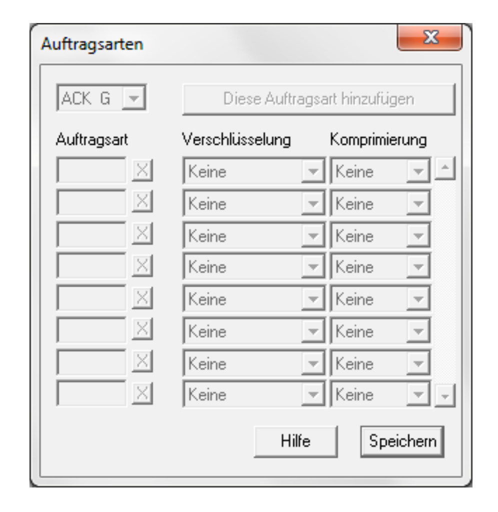


Angaben zum Status der Umstellung des EU-Verfahrens (noch nicht begonnen, kann beginnen, hat begonnen, fertig), zum Beginn der Umstellung und zur maximalen Dauer der Umstellungsphase (standardmäßig 60 Tage). Weitere Informationen dazu finden Sie in Kapitel 8.3: *Unterschriftsversion umstellen*.

Über die Schaltfläche [***DFÜ-Passwort ändern***] können Sie das Passwort, das in der BPD abgespeichert ist, ändern. (Das Passwort, das der Bank bekannt ist, wird hiermit nicht geändert! Dazu muss die Auftragsart PWA ausgeführt werden bzw. über -Kommunikation- / -DFÜ-Passwort ändern- [Assistent] das Passwort beim Bankrechner geändert werden.) Die Funktion muss dann genutzt werden, wenn eine FTAM-BPD aus einer Datensicherung zurückkopiert wurde, das Kontrollkästchen "DFÜ-Passwort speichern" gesetzt war und sich zwischen der Datensicherung und dem Rücksichern das DFÜ-Passwort geändert hat.
Jeder Benutzer kann dazu aus einer Liste der externen Namen ausgewählt werden. Sie geben einfach das neue Passwort ein. Da die Passworteingabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit wiederholen.
Sie bestätigen anschließend Ihre Eingaben mit <**Return**> oder durch Anklicken von [***Speichern***].

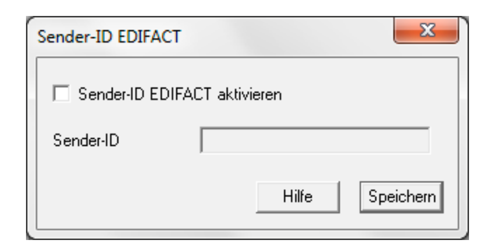


Über die Schaltfläche [***Auftragsarten***] legen Sie fest, für welche Auftragsarten eine Verschlüsselung bzw. eine Komprimierung mit FLAM ermöglicht werden soll. Die Angaben werden über die Auftragsart BPD "Bankparameter-Datei abholen" gefüllt, können aber auch von Ihnen editiert werden. Aus einer Auswahlliste aller möglichen Auftragsarten suchen Sie die von Ihnen gewünschte Auftragart aus. Diese jeweils markierte Auftragsart bringen Sie durch Drücken der Schaltfläche [***Diese Auftragsart hinzufügen***] in die darunter befindliche Tabelle. In dieser Weise verfahren Sie solange, bis sich alle von Ihnen gewüschten Auftragsarten in der darunterliegenden Tabelle befinden. Anschließend können Sie für jede einzelne Auftragsart gesondert festlegen, ob eine Verschlüsselung erfolgen soll oder nicht bzw. ob eine Komprimierung mittels FLAM stattfinden soll und bestätigen schließlich mit [***Speichern***].





Über die Schaltfläche [***Sender-ID EDIFACT***] können Sie, wenn Sie EDIFACT-Dateien versenden, diese mit einer sogenannten Sender-ID versehen.
Einige Banken erwarten bei EDIFACT-Übertragungen eine Unterschrift gemäß Sicherheits-Rahmenvertrag EDIFACT. Markieren Sie in diesem Fall das Optionsfeld "Sender-ID EDIFACT aktivieren" und setzen die Sender-ID in das entsprechende Feld ein. Führen Sie anschließend erneut eine Übertragung des öffentlichen Schlüssels an diese Bank durch (Auftragsart PUB).
Bitte beachten Sie, dass für EDIFACT-Übertragungen entweder ein EDIFACT-ZV-Modul oder die EDIFACT-Unterstützung installiert sein muss.



Eine Übertragung mit FTAM via Internet ist derzeit nicht möglich.

Durch Bestätigung über die Schaltfläche [***Speichern***] werden die Einstellungen in die jeweilige Bankparameterdatei übernommen.



3.4 FTP

FTP (**F**ile **T**ransfer **P**rotocol) ist ein Protokoll im Internet, das den Austausch von Dateien im Netz unterstützt.

Die Übertragung der Dateien erfolgt grundsätzlich im binären Modus. Eine Übertragung im ASCII-Modus ist nicht möglich, da alle Dateien in verschlüsselter Form übertragen werden.

Die Maske zur Pflege der FTP-BPD entspricht im wesentlichen der Maske zur Pflege der FTAM-BPD (s. Kapitel 3.3). Ebenfalls können bis zu 512 Unterschriftsberechtigte in einer BPD gespeichert werden (Zuordnung wie bei FTAM).

Bei den Verbindungsinformationen der Bank müssen Sie statt der Datex-P NUA bzw. der ISDN-NUA müssen Sie lediglich die **IP-Adresse** des Bank-Hostrechners sowie die Adressen des **Datenport**s (auf Bankseite) und des **Steuerport**s (auf Ihrer Seite) eintragen. Die Adressierung kann anstatt über die IP-Adresse auch mittels **DNS-Name** erfolgen. Dies erleichtert die Änderung der Adresse bei Umzug oder Providerwechsel.

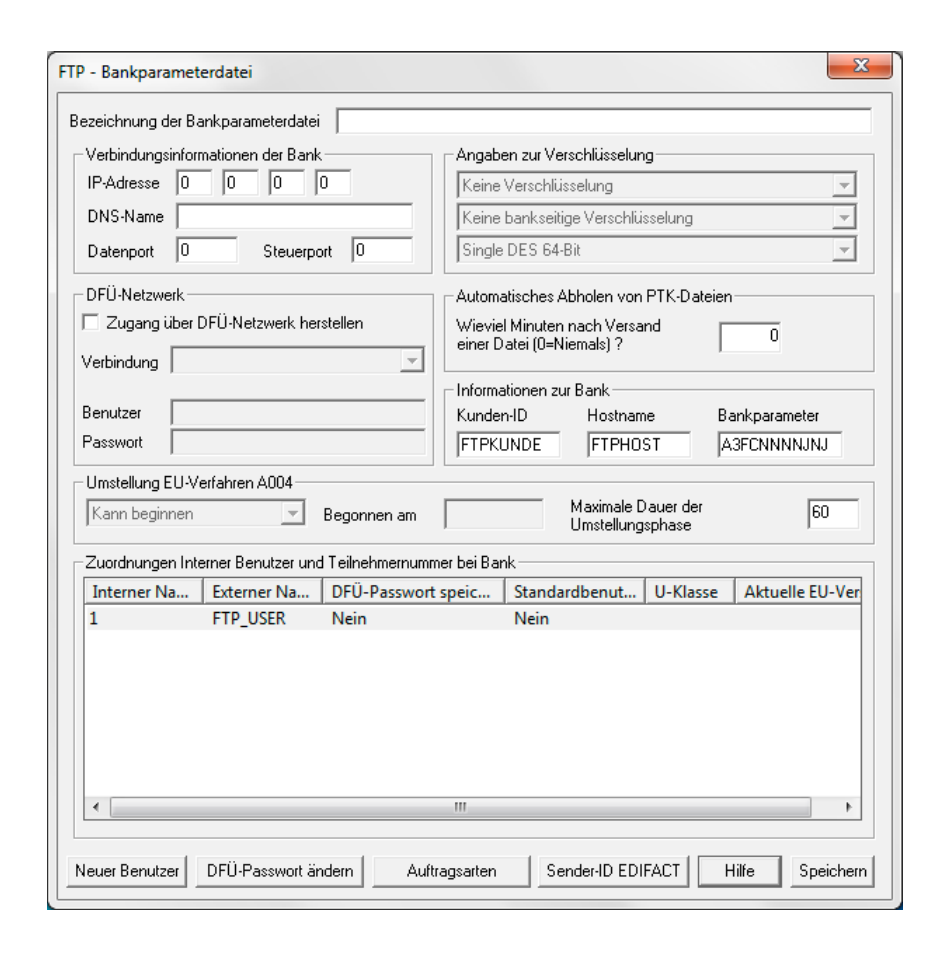
Zusätzlich gibt es Einstellmöglichkeiten zur Nutzung eines DFÜ-Netzwerkes.

Wenn Sie Ihren **Zugang über** das **DFÜ-Netzwerk herstellen** möchten, konfigurieren Sie bitte zuvor das DFÜ-Netzwerk von Windows und nehmen die notwendigen Einstellungen anhand der Angaben Ihres Internet-Providers vor. Wählen Sie Ihre **Verbindung** mittels der Auswahlliste aus und tragen **Benutzer** sowie **Passwort** ein.

Die sonstigen erforderlichen Angaben zur Konfiguration der Felder werden Ihnen von Ihrer Bank mitgeteilt.

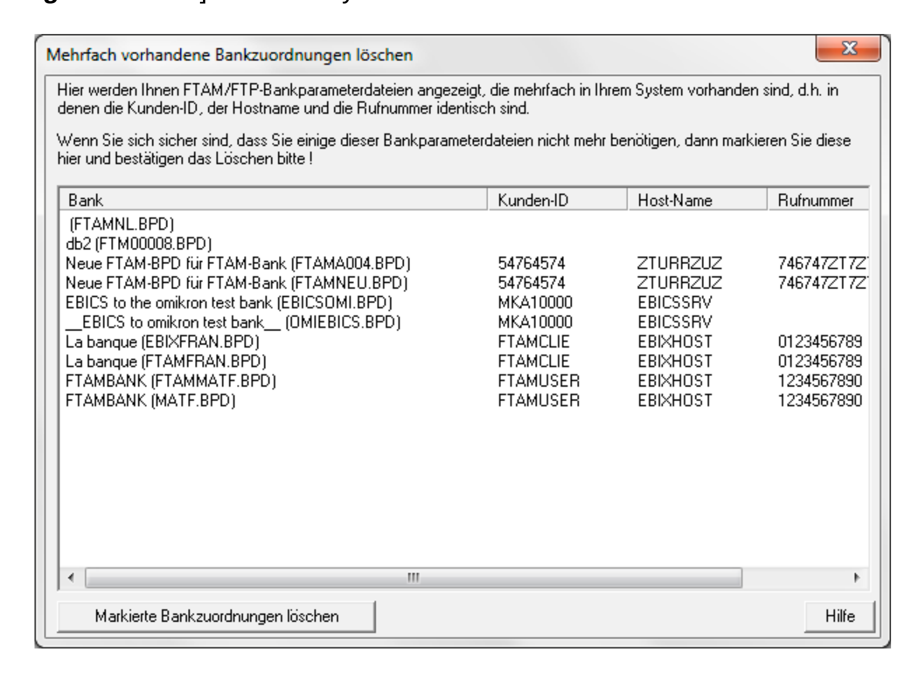
Im Zuge der Erhöhung des Signierschlüssels der EU auf eine Länge von 1024 Bit wurde auch für FTP der Bereich der Zuordnungen um eine Spalte mit der vom jeweiligen Teilnehmer verwendeten EU-Version erweitert (A003 oder A004). Unter "Umstellung EU-Verfahren A004" erfahren Sie Angaben zum Status der Umstellung des EU-Verfahrens (noch nicht begonnen, kann beginnen, hat begonnen, fertig), zum Beginn der Umstellung und zur maximalen Dauer der Umstellungsphase (standardmäßig 60 Tage). Weitere Informationen dazu finden Sie in Kapitel 8.3: *Unterschriftsversion umstellen*.





Mehrfach vorhandene Bankzuordnungen löschen (FTAM und FTP)

Sollten in Ihrem System FTAM- oder FTP-Bankparameterdateien entdeckt werden, die mehrfach vorhanden sind, d. h. die zwar vom Namen her unterschiedlich sind, in denen jedoch die Kunden-ID, der Hostname und die Rufnummer identisch sind, so werden Ihnen nach einer Neuinstallation diese Bankparameterdateien in einem besonderen Fenster angezeigt. Dort können Sie die nicht mehr benötigten Bankparameterdateien markieren und mittels der Schaltfläche [***Markierte Bankzuordnungen löschen***] aus dem System entfernen.



3.5 EBICS

EBICS (**E**lectronic **B**anking **I**nternet **C**ommunication **S**tandard) ist ein von allen deutschen Banken ab 2008 angebotenes Standardverfahren für die Kommunikation über das Internet. Ab November 2009 wird EBICS auch von allen Banken in Frankreich unterstützt (nur Version 2.4).

Wie bei der FTAM-/FTP-Kommunikation müssen Sie **für jede Bank eine gesonderte Bankparameterdatei** (BPD) erzeugen.

Wollen Sie einen bestehenden FTAM-/FTP-Zugang auf EBICS umstellen, verwenden Sie dazu bitte den Umstellungsassistenten unter -Kommunikation- / -FTAM-/FTP-Bankzugang auf EBICS umstellen- (Kapitel 4.6).

EBICS - Bankparameterdatei

Bezeichnung der Bankparameterdatei: EBICS mit Bankdaten

Verbindungsinformationen der Bank — ? — Adresse (URL): https://r-ufa3.tr.omikron.de/EBICS/ — Zugang prüfen

Authentifikationsstatus der Bank: Bereit

Informationen zur Bank — Kunden-ID: EBC323KK — Hostname: EBICSUFA — Betriebsmodus: Standard — Protokollversion: H004

Automatisches Abholen von PTK-Dateien — Wieviel Minuten nach Versand einer Datei (0=Niemals) ? 0

Zuordnungen Interner Benutzer und Teilnehmernummer bei Bank

Interner Name	Externer Name	DFÜ-Passwort speichern	Standardbenutzer	Aktuelle EU-Vers...	EBICS-Zustand
3	EBC323T3	Nein	Nein		Neu
2	EBC323T2	Nein	Nein		Neu
1	EBC323TT	Nein	Nein	A006	Bereit

Neuer Benutzer | DFÜ-Passwort ändern | Bankdaten | Hashwerte der Bank | EBICS-Parameter | Hilfe | Speichern

In einer EBICS-Bankparameterdatei stehen Ihnen die folgenden Felder zur Verfügung:

Bezeichnung der Bankparameterdatei

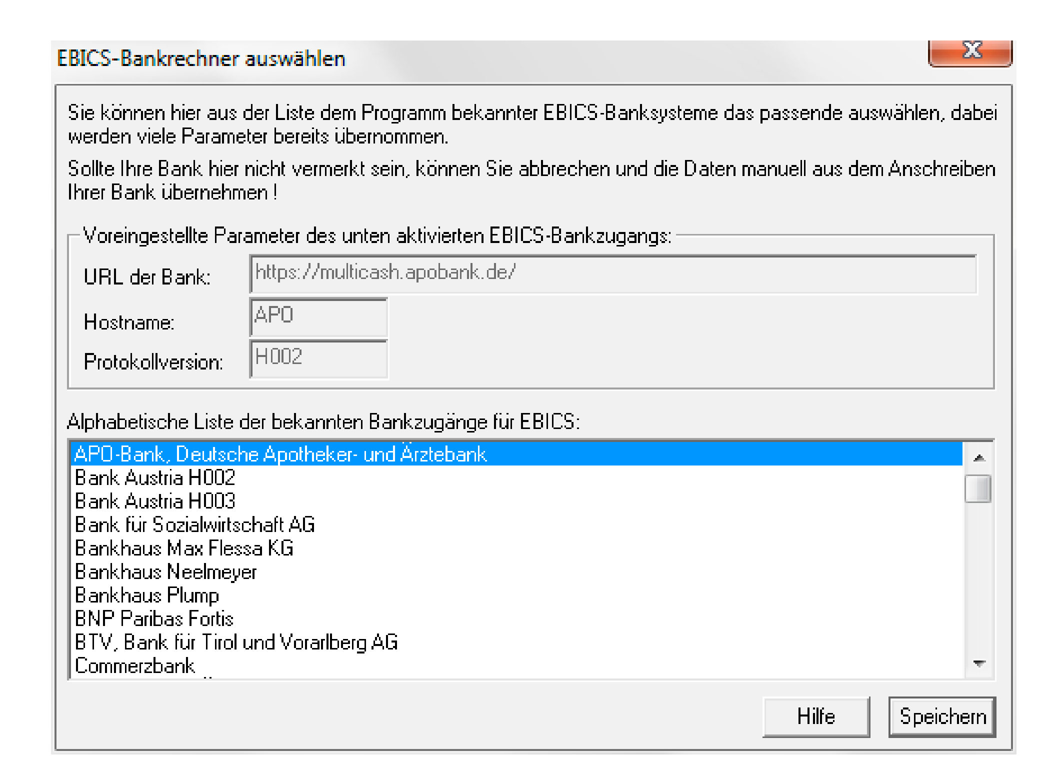
In dieses Feld tragen Sie eine aussagekräftige Bezeichnung der BPD ein (max. 30 Zeichen), die im weiteren Programmverlauf anstelle des Dateinamens der BPD verwendet wird.

Verbindungsinformationen der Bank:

Die erforderlichen Angaben werden Ihnen von Ihrer Bank mitgeteilt. Geben Sie hier die Internet-**Adresse (URL)** den Bankservers (DNS-Name bzw. IP-Adresse) für den EBICS-Zugang an.

Über die [**?**]-Schaltfläche vor den Verbindungsinformationen können Sie eine Liste bekannter EBICS-Bankzugangsdaten aufrufen.





Sofern ein passender Zugang in der alphabetischen Liste enthalten ist, können Sie diesen auswählen und die Zugangsdaten durch Betätigen der Schaltfläche [***Speichern***] in die Bankparameterdatei übernehmen.

Über die Schaltfläche [***Zugang prüfen***] können Sie eine Verbindungsprüfung zum Bank-Host vornehmen. Nach Drücken der Schaltfläche wird das Ergebnis der EBICS-URL-Prüfung entsprechend angezeigt. Schließen Sie das Fenster jeweils über die Schaltfläche [***OK***].

Es können folgende Meldungen angezeigt werden:

1. Im Falle eines falschen Zertifikates:
E_TLS_INVALID_CERTIFICATE- Es konnte keine erfolgreiche Verbindung hergestellt werden

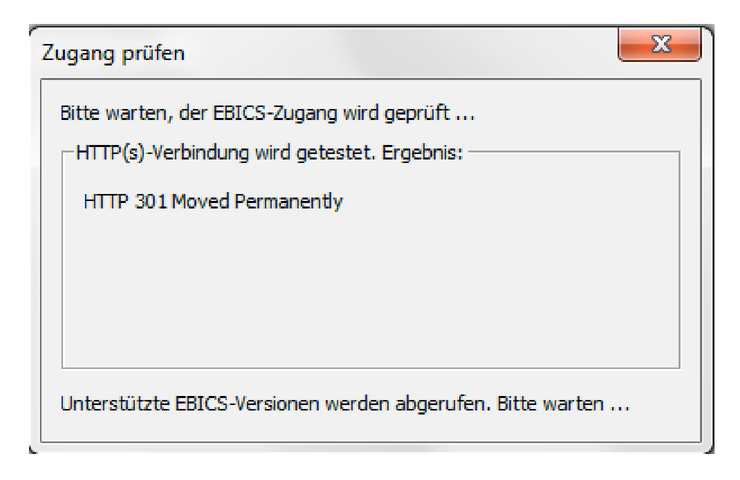
2. Im Fall, dass der Proxy mit falschem Port angesprochen wird:
E_TLS_INVALID_SERVER_HELLO - Es konnte keine erfolgreiche Verbindung hergestellt werden

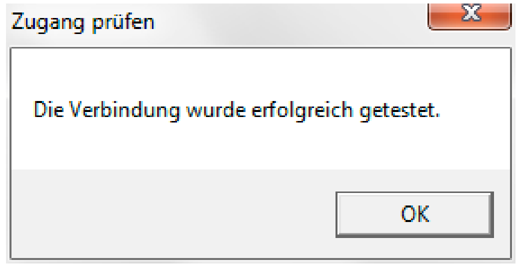
3. Im Fall, dass Proxy oder Server nicht gefunden werden:
E_HTTPCLIENT_CONNECT_FAILED - Es konnte keine erfolgreiche Verbindung hergestellt werden

4. Im Fall, dass der Server zwar gefunden wird, die Einstiegs-Seite aber falsch ist:
HTTP 404 Not Found- Die Verbindung wurde erfolgreich getestet

5. Im Fall, dass alles erfolgreich verläuft:
HTTP 301 Moved Permanently - Die Verbindung wurde erfolgreich getestet







Gleichzeitig wird ein **HEV-Abruf** (Unterstützte EBICS-Versionen) gestartet, der die vom Banksystem unterstützte EBICS-Protokollversion (siehe weiter unten) liefert (z. B. bei EBICS 2.4 die Protokollversion H003). Ist dieser Abruf erfolgreich, wird die Protokollversion in der BPD gesetzt und das Feld "EBICS-Protokollversion" gesperrt, da der Bankrechner ab dann die höchste zu verwendende EBICS-Version definiert (s. auch EBICS-Parameter weiter unten).

Über die Schaltfläche [***Zugang prüfen***] können bereits bestehende Bankzugänge manuell aktualisiert werden.
Dieser Abruf kann auch von noch nicht initialisierten Teilnehmern durchgeführt werden und ist daher ohne Authentifikationssignatur möglich. Der HEV-Abruf wird auch ausgeführt, wenn eine neu erfasste EBICS-BPD abgespeichert wird.

<u>Authentifikationsstatus der Bank:</u>

Hier finden Sie Angaben zum "**Authentifikationsstatus der Bank**", die entsprechenden Angaben zum Teilnehmerstatus finden sich weiter unten im Bereich der Teilnehmerzuordnung. Zunächst finden Sie hier die Statusangabe "Neu" (vor Abruf der Bankschlüssel). Nach erfolgreicher Verifikation der Schlüssel ändert sich die Angabe auf "Bereit". Ein Scheitern der Verifikation wird angezeigt durch "Verifikation fehlerhaft".

<u>Informationen zur Bank:</u>

Die bankseitig definierte **Kunden-ID** dient bei allen DFÜ-Aufträgen der Identifizierung des Kunden. Der Bankrechner akzeptiert Ihre DFÜ-Aufträge nur, wenn Sie bei Ihrer Bank über eine Kunden-ID verfügen. Den **Hostname**n bekommen Sie von Ihrer Bank mitgeteilt.

Über das Feld **Betriebsmodus** wird definiert, mit welcher EBICS-Variante die Bank arbeitet, z. B. Standard, Frankreich T (Transport EU), Frankreich TS (persönliche EU), Schweiz UBS.

Unter **EBICS-Protokollversion** wird die von der Bank unterstützte Protokollversion angezeigt. Nach einem HEV-Abruf wird die vom Banksystem unterstützte Protokollversion hier eingetragen.

Hierdurch ist sichergestellt, dass die Initialisierung mit der höchsten von beiden Systemen unterstützten Protokollversion durchgeführt wird. Schlägt der Abruf fehl, wird in die BPD-Datei die Version H002 eingetragen (da dies immer funktionieren muss).



Automatisches Abholen von PTK-Dateien:

Wenn Sie hier hinter dem Feld: "Wieviel Minuten nach Versand einer Datei?" die Vorbelegung 0 durch eine Zahl ersetzen, erfolgt nach der entsprechenden Zeit **nach** einem EBICS-Sendeauftrag ein automatisches Abholen der zugehörigen Protokollinformationen. Bei "0" erfolgt kein automatisches Abholen.

Für die Art des Kundenprotokolls gilt Folgendes:

Auftrags-art	**Protokoll-version**	**Betriebsmodus**	**Bemerkung**
PTK	Alle	Alle	Wird in Frankreich teilweise nicht komplett unterstützt.
ACK	H003	Frankreich T und TS	Ist in den EBICS-Parametern der Parameter "Payment Status Report statt Kundenprotokoll?" (s. unten) gesetzt, wird für H003 automatisch ACK ausgeführt.
HAC	Ab H004	Alle	Ist in den EBICS-Parametern der Parameter "Payment Status Report statt Kundenprotokoll?" (s. unten) gesetzt, wird für H004 automatisch **HAC** ausgeführt (EBICS-Kundenprotokoll im XML-Format).

Zuordnungen Interner Benutzer und Teilnehmernummer bei der Bank:

Zusätzlich zur Kunden-ID legen Sie interne und externe Namen für die einzelnen Anwender fest, die mit der jeweiligen BPD arbeiten dürfen. Bis zu 512 Unterschriftsberechtigte können in einer BPD gespeichert werden.

Die bankseitig definierten "**externen Namen**" erhalten Sie von Ihrer Bank. Jeder Kunden-ID können mehrere externe Namen zugeteilt werden.
Die externen Namen können von Ihnen bestimmten Benutzern zugeteilt werden. Unter "**interner Name**" können Sie über ein Listenfeld aus den im Menüpunkt -Benutzer- definierten Benutzernamen wählen. Nur die unter "interner Benutzer" eingetragenen Benutzer, denen ein "externer Name" zugeteilt wurde, können Daten via EBICS mit einer Bank austauschen.

Über die Schaltfläche [***Neuer Benutzer***] bzw. den Kontextmenüeintrag -Neuaufnahme Benutzer- beim Klick mit der rechten Maustaste auf einen bereits erfassten Benutzer können neue Benutzer (aus dem am Rechner verfügbaren Benutzern) ausgewählt werden und in die BPD aufgenommen werden (ein neuer Datensatz wird angelegt). Durch Anklicken mit der linken Maustaste in der Auflistung bzw. über den Kontextmenüeintrag -Datensatz pflegen- (rechte Maustaste) können bestehende Datensätze editiert werden. Über -Löschen- und Bestätigen der Sicherheitsabfrage mit [***Ja***] können Benutzereinträge aus der BPD entfernt werden.
Zusätzlich zum externen Namen kann für jeden Benutzer festgelegt werden, ob das DFÜ-Passwort in der Bankparameterdatei gespeichert werden soll. Dazu wählen Sie in der Spalte "**DFÜ-Passwort speichern**" aus der Liste entweder "Ja" oder "Nein". Weiterhin können Sie bestimmen, ob es sich bei dem erfassten Benutzer um einen "**Standardbenutzer**" handeln soll. Nähere Informationen finden Sie im Text zum Umstellungsassistenten, wo Sie im Rahmen der Umstellung einen Anwender als Standardbenutzer (Technischer Benutzer) definieren können (s. Kapitel 4.6: *FTAM/FTP-Bankzugang auf EBICS umstellen*: Standardbenutzer definieren).
Die Informationen zur verwendeten Elektronischen Unterschrift (**Aktuelle EU-Version**; EBICS setzt auf der Unterschriftsversion A004 auf) und zum **EBICS-Zustand** für jeden Benutzer (zum Authentifikationsstatus der Bank s. oben) werden im Rahmen des Datenaustausches mit der Bank aktualisiert. Mögliche Zustände für den Benutzer sind:

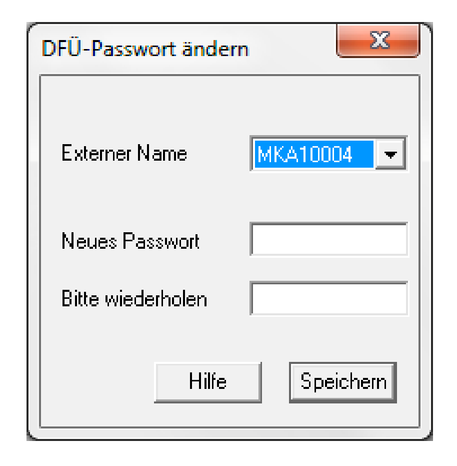
Neu - vor Initialisierung
Teilweise initialisiert (INI) - wenn nur INI erfolgreich durchgeführt wurde
Teilweise initialisiert (HIA)- wenn nur HIA erfolgreich durchgeführt wurde



Bereit - wenn INI und HIA erfolgreich durchgeführt wurden
Gesperrt - wenn ein SPR-Auftrag erfolgreich durchgeführt wurde

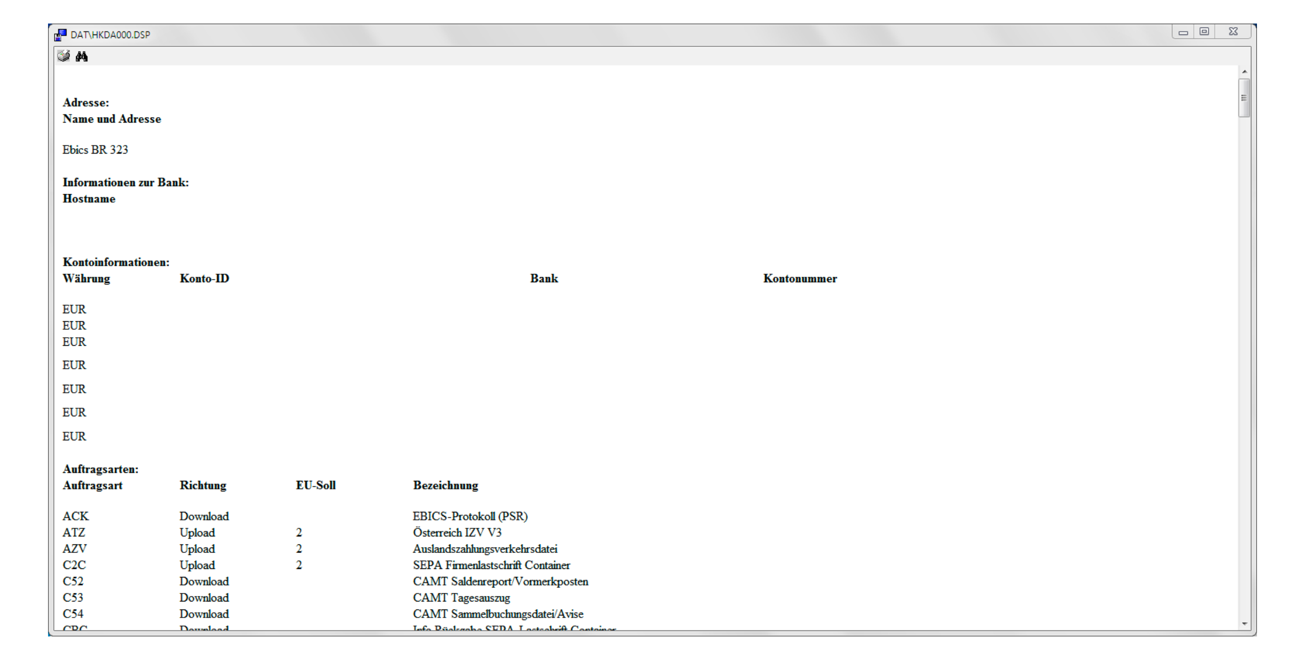
Weitere Funktionsschaltflächen:

Über die Schaltfläche [***DFÜ-Passwort ändern***] können Sie das Passwort, das in der BPD abgespeichert ist, ändern. Jeder Benutzer kann dazu aus einer Liste der **externen Namen** ausgewählt werden. Sie geben einfach ein **neues Passwort** ein. Da die Passworteingabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit **bitte wiederholen**.



Abschließend bestätigen Sie Ihre Eingaben mit <**Return**> oder durch Anklicken von [***Speichern***].

Mit dem monatlichen HPD-Abruf (Bankparameter abholen) wird auch ein **HKD-Abruf** (Kunden- und Teilnehmerinformationen abholen) durchgeführt. Die empfangenen Daten werden je Bankparametersatz abgelegt und können über die Schaltfläche [***Bankdaten***] angezeigt werden. Wird der Abruf manuell über den Dateimanager durchgeführt, werden die Daten beim jeweiligen Auftrag angezeigt [auch für **HTD-Aufträge** (Teilnehmerinformationen abholen)]. Dort ist auch jederzeit eine manuelle Aktualisierung möglich.





Die Schaltfläche [***Hashwerte der Bank***] dient zur Anzeige der zuletzt eingegebenen Hashwerte (**Authentifikationshash der Bank (X0??)** / **Verschlüsselungshash der Bank (E0??)**) bzw. zum Abgleich mit den von der Bank abgeholten Schlüsseln (Sessiontyp HPB). Die Hashwerte werden Ihnen von der Bank mitgeteilt.

Sie müssen nicht alle Werte eingeben. Normalerweise reichen zur Authentifizierung wenige Stellen aus. Alle von Ihnen eingegebenen Werte werden mit den übermittelten Werten abgeglichen. Beenden Sie die Eingabe durch Drücken der [***Speichern***]-Schaltfläche.
Nähere Informationen finden Sie im Text zum Umstellungsassistenten, wo Sie im Rahmen der Umstellung bereits die Hashwerte eingeben können (s. Kapitel 4.6: *FTAM/FTP-Bankzugang auf EBICS umstellen*: Hashwerte der Bankschlüssel eingeben).

Nach Abholung der Bankschlüssel mittels Auftragsart HPB sind die Hashwerte der Bank hier eingetragen und die Maske ist nicht mehr editierbar.
War der Abgleich der Hashwerte nicht erfolgreich, bleiben diese editierbar und können nach dem manuellen Abgleich über die Schaltfläche [***Freigabe der Hashwerte***] freigegeben werden.

Hashwerte der Bank

Authentifikationshash der Bank (X0??)

Stellen 1-8:	DB	FE	12	39	B4	CB	EA	E7
Stellen 9-16:	67	D1	C	A8	5C	8F	5E	50
Stellen 17-24:	D8	52	5C	5B				
Stellen 25-32:								

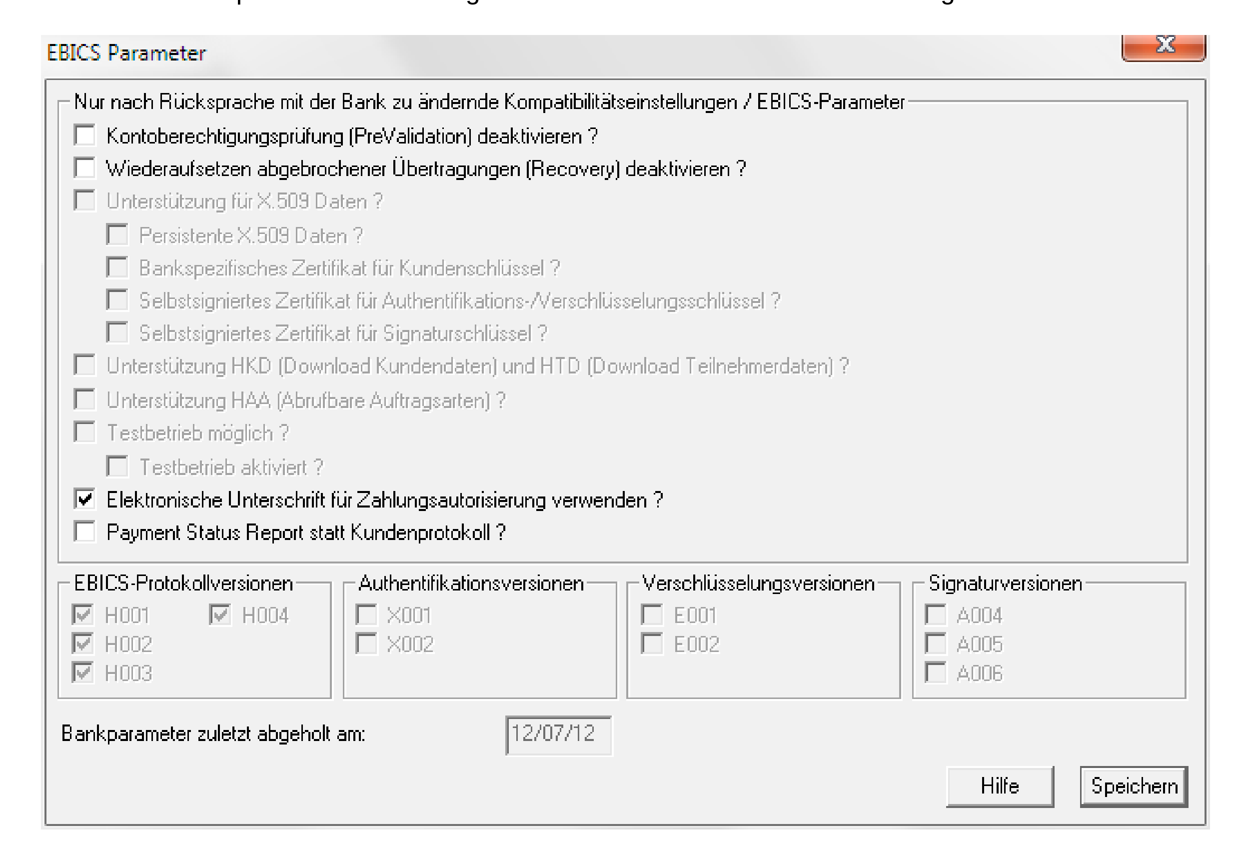
Verschlüsselungshash der Bank (E0??)

Stellen 1-8:	DB	FE	12	39	B4	CB	EA	E7
Stellen 9-16:	67	D1	C	A8	5C	8F	5E	50
Stellen 17-24:	D8	52	5C	5B				
Stellen 25-32:								

Freigabe der Hashwerte | Hilfe | Speichern



Über die Schaltfläche [***EBICS-Parameter***] erreichen Sie eine Übersicht, in der die von der Bank unterstützten Kompatibilitätseinstellungen/Parameterinformationen zusammengefasst sind.



Kompatibilitätseinstellungen/EBICS- Parameter:

Achtung! Die Einstellungen in diesem Abschnitt sind jeweils nur nach Rücksprache mit der Bank zu ändern:

Die Funktion "**PreValidation**" sorgt dafür, dass immer alle zur Vorab-Prüfung von EU, Kontoberechtigung und Limit notwendigen Informationen mit übertragen werden. Unterstützt das Banksystem die Funktion "PreValidation", wird bei gescheiterter Vorab-Prüfung die Rückmeldung des Bankservers im Dateimanager angezeigt. Der Auftrag kann dann erneut bearbeitet werden.
Durch Markieren des Kontrollkästchens "**Kontoberechtigungsprüfung (PreValidation) deaktivieren?**" kann diese Funktion kundenseitig bei Bedarf abgeschaltet werden.

Die Funktion "**Recovery**" ermöglicht es, die Übertragung eines Auftrages nach einem Kommunikationsabbruch fortzusetzen, ohne alle bereits erfolgreich versandten Auftragsdatensegmente erneut übertragen zu müssen. Unterstützt das Banksystem ebenfalls die Funktion "Recovery" wird bei der Wiederholung die Kommunikation automatisch am Wiederaufsetzpunkt fortgesetzt.
Durch Markieren des Kontrollkästchens "**Wiederaufsetzen abgebrochener Übertragungen (Recovery) deaktivieren?**" kann diese Funktion kundenseitig gegebenenfalls abgeschaltet werden.

Sofern die Bank die Verwendung von Zertifikaten unterstützt, ist das Kontrollkästchen "**Unterstützung für X.509-Daten?**" markiert. In Frankreich sind Zertifikate für Kunde und Bank Pflicht.
Zusätzlich kann das das Kontrollkästchen "**Persistente X.509-Daten?**" markiert sein.

Weitere Optionen sind:
"**Bankspezifisches Zertifikat für Kundenschlüssel?**". Hierüber besteht die Möglichkeit, für einen privaten Schlüssel ein Zertifikat je Bank zu unterstützen.



"**Selbstsigniertes Zertifikat für Authentifikations-/Verschlüsselungsschlüssel?**". In diesem Fall ist keine CA nötig (in Frankreich Standard).
"**Selbstsigniertes Zertifikat für Signaturschlüssel?**" In Frankreich bei der Variante T.

Sofern die Bank die Funktion "ClientDataDownload" unterstützt, ist das entsprechende Kontrollkästchen markiert. Dabei werden die Auftragsarten **HKD** (**Download Kundendaten**) und **HTD** (**Download Teilnehmerdaten**) verwendet.

Sofern die Bank den Abruf von Auftragsarten unterstützt, ist das Kontrollkästchen "**Unterstützung HAA**" (Abrufbare Auftragsarten abholen) markiert.

Sofern die Bank die Option EBICS-Testbetrieb unterstützt, ist das Kontrollkästchen "**Testbetrieb möglich?**" markiert (in Frankreich Standard). Der Testbetrieb wird über das nachfolgende Kontrollkästchen "**Testbetrieb aktiviert?**" aktiviert bzw. deaktiviert.

Weitere Optionen sind:

"**Elektronische Unterschrift für Zahlungsautorisierung verwenden?**".
Über diese Option wird gesteuert, ob mit dieser Bank Elektronische Unterschriften zur Zahlungsautorisierung genutzt werden sollen. Ist der Schalter nicht aktiviert, kann die Datei zwar im Zahlungsverkehrsmodul unterschrieben werden, wird aber mit Attribut T (Transportunterschrift) in den Dateimanager eingestellt.

"**Payment Status Report statt Kundenprotokoll?**".
Ist diese Option markiert, wird in Abhängigkeit von der Protokollversion (s. oben) statt des Kundenprotokolls (Auftragsart PTK) ein Payment Status Report abgeholt (Auftragsart ACK bzw. HAC).

<u>EBICS- Protokollversionen:</u>
Die von der Bank unterstützte EBICS-Protokollversion wird hier eingetragen. Mit der EBICS-Version 2.4/2.5 wurde eine neue Protokollversion (H003/H004) eingeführt.

<u>Authentifikationsversionen:</u>
Die von der Bank unterstützte Version des Authentifikationsverfahrens wird hier eingetragen. Mit der EBICS-Protokollversion H003 wurde auch eine neue Version des Authentifikationsverfahrens (X002) eingeführt.

<u>Verschlüsselungsversionen:</u>
Die von der Bank unterstützte Version des Verschlüsselungsverfahrens wird hier eingetragen. Mit der EBICS-Protokollversion H003 wurde auch eine neue Version des Verschlüsselungsverfahrens (E002) eingeführt.

<u>Signaturversionen:</u>
Die von der Bank unterstützte Signaturversion wird hier eingetragen. Mit der EBICS-Protokollversion H003 wurden die EU-Versionen A005 und A006 neu eingeführt.

Die Aktualisierung der unterstützten Features der Bank erfolgt einmal monatlich automatisch mittels **HPD-Abruf** (Bankparameter abholen). Das Datum des letzten HPD-Abrufes wird in der BPD gespeichert und hier unter "**Bankparameter zuletzt abgeholt am:**" angezeigt. Bei jeder Kommunikation wird geprüft, ob der letzte HPD-Abruf einen Monat oder länger zurück liegt. Ist dies der Fall (oder ist noch gar kein letztes Abrufdatum gespeichert), wird automatisch vor dem anstehenden Auftrag ein HEV- und ein HPD-Abruf durchgeführt und das Datum hier eingetragen.



 **Bitte beachten Sie ...**

Möchten Sie einen HPD-Abruf außerhalb der festen Monatstermine durchführen, zum Beispiel "auf Zuruf" einer Bank, so ist dies jederzeit im Datei-Manager durch Anlegen eines Abholauftrages möglich.

Durch abschließendes Bestätigen mit der Schaltfläche [***Speichern***] werden die Einstellungen in die EBICS-Bankparameterdatei übernommen.



3.6 HBCI

Beim HBCI-Verfahren (Homebanking Computer Interface) arbeiten Sie mit einem individuellen digitalen Schlüssel auf einer persönlichen Diskette oder Chipkarte. Diese schieben Sie während der Arbeit mit dem Programm in das Diskettenlaufwerk bzw. in einen speziellen Chipkartenleser. Mit Hilfe der Daten auf der Diskette oder auf der Chipkarte werden nach Eingabe eines Passwortes/einer PIN Ihre Aufträge an die Bank verschlüsselt.

Zur Nutzung von HBCI müssen Sie unabhängig vom verwendeten Sicherheitsmedium dafür sorgen, dass

- das "Kommunikationsmodul HBCI" installiert wurde.
- über den Menüpunkt -Kommunikation- / -DFÜ-Parameter- auf der *Registerkarte Prioritäten* das Verfahren "TCP/IP-Verbindung" angeklickt wurde. Auf der *Registerkarte TCP/IP-Verbindung* ist dann einzustellen, ob die Verbindung über ein DFÜ-Netzwerk oder LAN erfolgt.

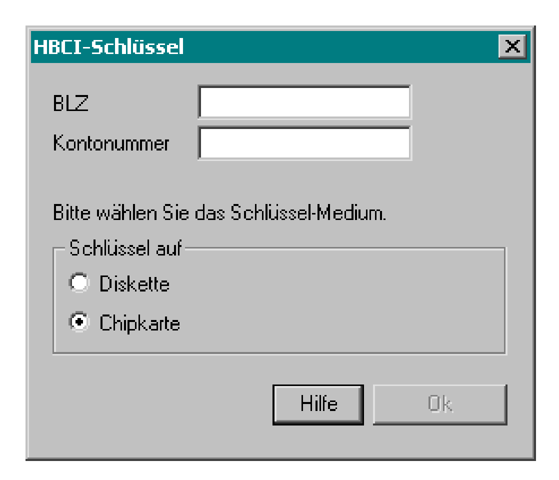
Sollten Sie das HBCI-Verfahren *mit Chipkarte* nutzen wollen, müssen Sie zusätzlich sicherstellen, dass

- der zum Chipkartenleser gehörende Treiber installiert wurde,
- der angeschlossene Chipkartenleser über den Menüpunkt -Chipkartenleser- in der Windows-Systemsteuerung getestet wurde.

Nach Drücken der Schaltfläche [***Neue BPD***] unter -Kommunikation- /-Bankparameterdateien-, Auswahl des Verfahrens "HBCI" über die Auswahlliste und Eingabe eines Namens für die Bankparameterdatei öffnet sich ein Dialog zur Eingabe der Kontoverbindung und Auswahl des Schlüsselmediums.



Der interne BPD-Dateiname darf maximal 8 Stellen haben und nur aus den Zeichen (A-Z,a-z,0-9,-,_) bestehen.



Geben Sie zunächst in die beiden Eingabefelder Ihre Kontoverbindung bestehend aus Bankleitzahl (**BLZ**) und **Kontonummer**, für die Sie das Verfahren HBCI nutzen wollen, ein. Anschließend wählen Sie das Medium zur Speicherung der Schlüssel durch Anklicken der entsprechenden Option aus.

Das weitere Vorgehen unterscheidet sich dabei etwas je nach Nutzung von **Diskette** oder **Chipkarte**:

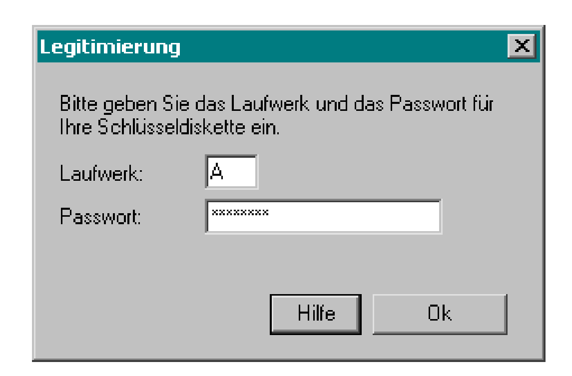


Alternative A: Sie wollen eine Schlüsseldiskette nutzen...

Nach Bestätigen der Auswahl mit [***OK***] geben Sie im folgenden Dialog nacheinander ein:

- das **Laufwerk** (den Laufwerksbuchstaben) für Ihre HBCI-Schlüsseldiskette
  Ein Schlüsselpaar besteht aus einem Private Key (Privater Schlüssel) und einem Public Key (Öffentlicher Schlüssel). Der Private Key kann nur auf eine Diskette geschrieben werden. Daher ist im ersten Eingabefeld nur die Eingabe von "A" oder "B" zulässig.
  Der Public Key wird auf der Festplatte abgespeichert und per Datenfernübertragung zur Bank geschickt.
- das ab sofort zu nutzende **Passwort** (PIN / Passphrase)

Mit der PIN / Passphrase greifen Sie bei jeder Interaktion mit der Bank (Schlüsselwechsel, Versenden eines Zahlungsauftrages, Abholen von Kontoinformationen etc.) auf den auf der Diskette hinterlegten Private Key zu.

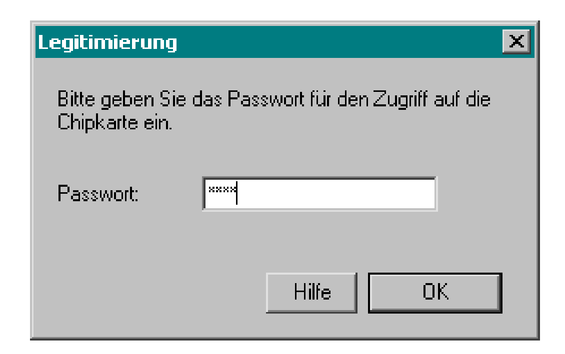


Nach Bestätigen mit [***OK***] öffnet sich die Eingabemaske für die Daten der Bankparameterdatei.

Alternative B: Sie wollen eine Chipkarte nutzen...

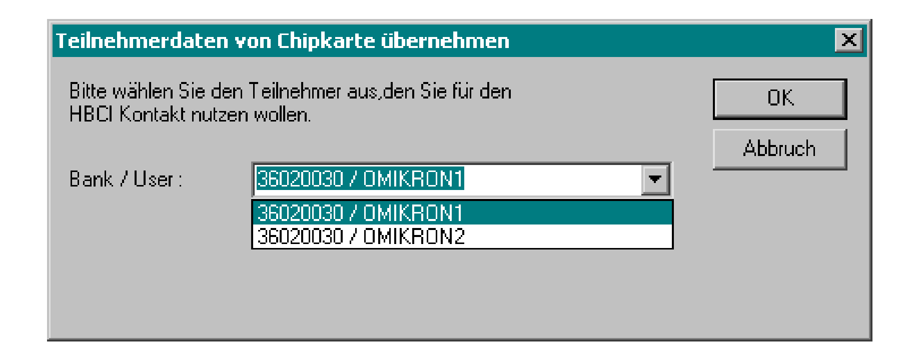
- Nach Bestätigen der Auswahl mit [***OK***] legen Sie nach Aufforderung durch das Programm Ihre Chipkarte in den **Chipkartenleser** ein.

- Anschließend geben Sie Ihr **Passwort** (PIN / Passphrase) ein.
  Mit der PIN / Passphrase greifen Sie bei jeder Interaktion mit der Bank (Schlüsselwechsel, Versenden eines Zahlungsauftrages, Abholen von Kontoinformationen) auf den auf der Chipkarte hinterlegten Private Key zu.



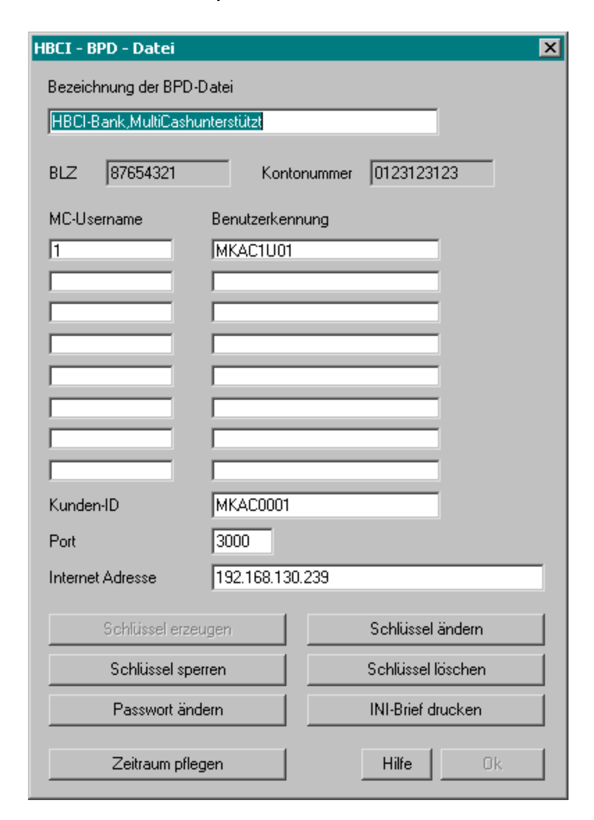
Haben Sie von Ihrer Bank eine vorkonfigurierte Chipkarte erhalten, folgt eine weitere Abfrage zur Übernahme der Daten.





Nach Auswahl und Bestätigen mit [***OK***] sind die entsprechenden Daten dann bereits in der folgenden Maske der HBCI-Bankparameterdatei eingetragen.

Nach der jeweiligen Auswahl des Schlüsselmediums und Legitimierung mittels Passwort öffnet sich die Eingabemaske für die Daten der HBCI-Bankparameterdatei:



Wenn die Zugangsdaten auf Diskette abgelegt werden sollen, erhalten Sie von Ihrem Kreditinstitut ein Schriftstück (Erstzugangsbrief), das die wesentlichen Daten für Ihren HBCI-Zugang enthält. Ein Beispiel dazu finden Sie hier. Bei Übersendung einer Chipkarte kann dieses Schriftstück entfallen (Feldeinträge werden von der Chipkarte übernommen) bzw. nur einen Teil der im Beispiel enthaltenen Informationen aufweisen (um die die übernommenen Einträge dann noch ergänzt werden müssen).

Die Ihnen mitgeteilten Daten tragen Sie in die Felder der Dialogbox ein; liegen Ihnen zusammen mit Ihrer Chipkarte keine solchen schriftlichen Informationen vor, dann sind diese komplett auf Ihrer Chipkarten enthalten. In diesem Fall bestätigen Sie die Dialogbox einfach über die Schaltfläche [***OK***].

☞ **Bitte beachten Sie ...**

Selbstverständlich können zu einem Konto auch mehrere Benutzer zugriffsberechtigt sein (weitere Einträge unter MC-Username und Benutzerkennung). In diesem Fall müssen die entsprechenden Benutzerdaten ebenfalls hinterlegt werden und jeder weitere eingetragene

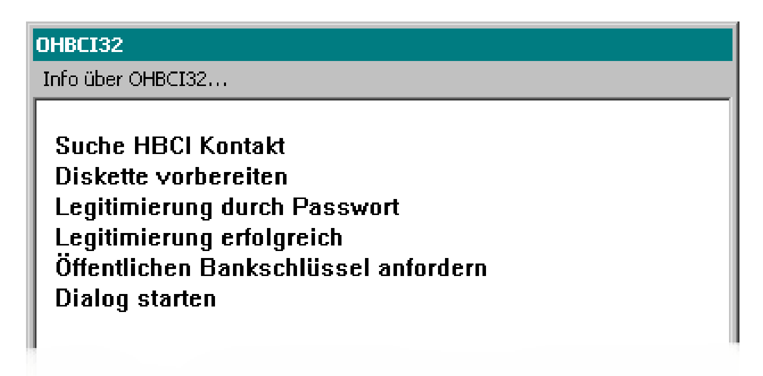


Benutzer muss sich zu einem späteren Zeitpunkt beim System neu anmelden, unter -Kommunikation- /-Bankparameterdateien- die HBCI-Datei auswählen, sich legitimieren und die nachfolgend beschriebene Prozedur mit seinem eigenen Sicherheitsmedium durchführen.

Bei neuen Schlüsselmedien ist zunächst nur die Schaltfläche [***Schlüssel erzeugen***] aktiv.



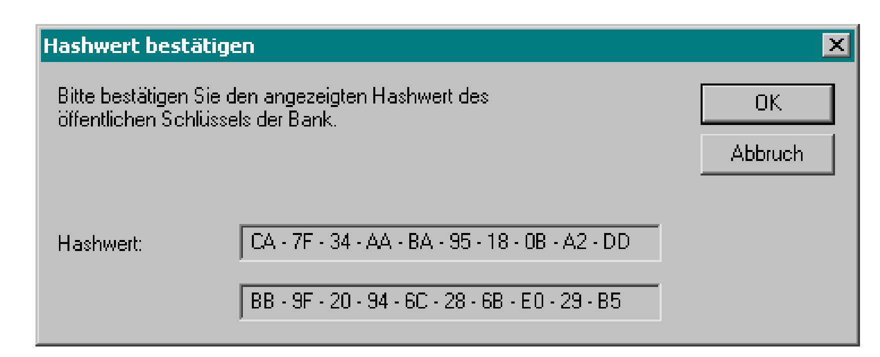
Tragen Sie die von den Bank mitgeteilten Angaben zu Ihrem HBCI-Zugang in die entsprechenden Felder ein und starten Sie dann die Schlüsselpaar-Generierung für den aktuell angemeldeten Benutzer (!) durch Betätigen der Schaltfläche [***Schlüssel erzeugen***].



Übrigens:

Während der Erstellung der Signier- und Chiffrierschlüssel wird gleichzeitig auch Kontakt mit dem jeweiligen Kreditinstitut aufgenommen. Die dort vorgehaltenen Bankschlüssel, die ebenfalls zur Kommunikation erforderlich sind, werden - sofern sie nicht schon auf der Chipkarte gespeichert sind - abgeholt und stehen dann zur weiteren Nutzung im Programm zur Verfügung.

Wurde der öffentliche Schlüssel der Bank erfolgreich abgeholt, müssen Sie anschließend den in einem weiteren Dialog angezeigten Hashwert mit den schriftlich übermittelten Daten der Bank (ein Beispiel hierzu finden Sie hier) vergleichen und die Übereinstimmung mit [***OK***] bestätigen.





Nach erfolgreicher Schlüsselpaarerstellung und Austausch des öffentlichen Schlüssels des aktuellen Benutzers sind nun auch die weiteren Schaltflächen auf der Maske der HBCI-Bankparameterdatei aktiv. Jetzt sollten Sie über die Schaltfläche [***INI-Brief drucken***] den Initialisierungsbrief (mit Ihrem öffentlichen Schlüssel) ausdrucken (Datei: PINBRIEF.TXT), den Sie zur Freischaltung Ihres HBCI-Zuganges unterschrieben an die Bank schicken müssen.



<u>Beispiel</u>: Initialisierungsbrief des Teilnehmers (Benutzers, Users)

```
I N I T I A L I S I E R U N G S B R I E F


Benutzername          1
Datum                 30.09.03
Uhrzeit               13:47
Empfänger             87654321
Benutzerkennung       MKAC1U01
KundenID              MKAC0001
Schlüsselnummer       1
Schlüsselversion      1
HBCI-Version          210

Öffentlicher Schlüssel für die elektronische Signatur

Exponent

00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00

Modulus

00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
B6 9C FE 78 - 20 6B 93 47 - 10 D3 F2 8F - 41 20 E6 DF
30 FF 4B B1 - 98 AF A5 06 - 15 BD 1B 0f - C9 BB 1C 96
F3 35 62 4B - 8E E8 E7 8B - 3A 41 22 67 - 85 AC B8 CD
65 32 D8 88 - F0 D3 07 8A - A7 03 CD 5D - 39 80 A6 58
00 B7 3A 0e - EF 47 3C B7 - CD CB F4 BE - E7 4A F2 38
53 0d 4E 4E - DF 97 38 3D - D6 DA 7E E7 - 76 CB A9 75

Hash          5B AD 1C 27 - 3B 68 7C 83 - 6C 15
              34 21 69 C7 - 1A AA 2B B5 - 98 0E


Hiermit wird der obige öffentliche Schlüssel für die Elektronische Unterschrift
des unter der obigen Benutzerkennung berechtigten Nutzers bestätigt.

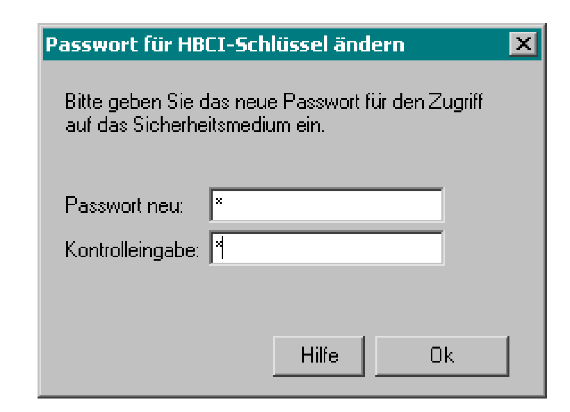

________________________         ________________________

        Ort/Datum                        Unterschrift
```

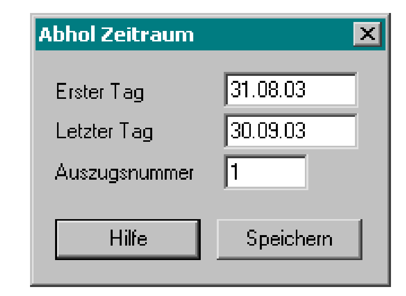
Bei Bedarf können Sie dann in der Maske der HBCI-Bankparameterdatei über die entsprechenden Schaltflächen Ihre [***Schlüssel ändern***], [***Schlüssel sperren***] oder [***Schlüssel löschen***].

Über die Schaltfläche [***Passwort ändern***] können Sie das Passwort für den Zugriff auf Ihr Schlüsselmedium ändern. Geben Sie dazu das neue Passwort in das entsprechende Feld ein. Im Feld Kontrolleingabe wiederholen Sie Ihre Eingabe zur Sicherheit noch einmal.





Über die Schaltfläche [***Zeitraum pflegen***] können Sie analog zu HBCI+ (vgl. Kapitel 3.7.1*: Zeitraum pflegen*) den Abholzeitraum sowie die "Start"-Auszugsnummer von Kontoauszügen bei Bedarf abändern.



Eine "Zeitraum-Pflege" ist nur dann erforderlich, wenn Sie die vom Programmsystem vergebenen Standardeinstellungen verändern wollen.

Nach Aufruf der Schaltfläche [***Zeitraum pflegen***] erscheint eine Eingabemaske , in der das Feld "Erster Tag" das aktuelle Systemdatum - 1 Monat und das Feld "Letzter Tag" das aktuelle Systemdatum enthalten; das Feld "Auszugsnummer" ist mit 1 vorbelegt.

Sollen die Kontoinformationen zu einem anderen Anfangszeitpunkt und/ oder mit einer anderen "Start"-Auszugsnummer abgeholt werden, müssen Sie die Vorgabe entsprechend abändern.

Die Angabe eines Anfangszeitpunktes ist nur dann erforderlich, wenn Sie bisher noch keine Kontoinformationen bei Ihrer Bank abgeholt haben.

Im weiteren Programmverlauf wird das Datum im Feld "Letzter Tag" immer auf das aktuelle Systemdatum gesetzt. Im Feld "Erster Tag" wird immer das letzte Auszugsdatum + 1 Tag eingetragen. (Ausnahme: Beim letzten Abholvorgang wurde festgestellt, dass die abgeholten Kontoinformationen nicht vollständig sind. In diesem Fall lässt das Programm das Datum "Erster Tag" unverändert, damit beim nächsten Abholvorgang auch die noch fehlenden Daten übertragen werden können.)

Ist bereits ein Auszug für die in der BPD eingetragene Bankleitzahl mit der von Ihnen manuell eingetragenen Auszugsnummer in den Datenbanken des Cashmanagement-Moduls gespeichert, so wird dieser Auszug überschrieben. Achten Sie daher immer auf die korrekte Eingabe der "Start"-Auszugsnummer.

Im weiteren Programmbetrieb wird die Auszugsnummer nach jedem Abholvorgang um 1 erhöht. (Ausnahme: Beim letzten Abholvorgang wurde festgestellt, dass die abgeholten Kontoinformationen nicht vollständig sind. In diesem Fall lässt das Programm die Auszugsnummer unverändert, damit beim nächsten Abholvorgang auch die noch fehlenden Daten übertragen werden können.)

Sie übernehmen Ihre Einstellungen durch Betätigen der Schaltfläche [***OK***].



Um das Kommunikationsverfahren HBCI nutzen zu können, müssen Sie sicherstellen, dass Sie die erzeugte HBCI-Bankparameterdatei unter -Hilfsdatenbanken- / -Banken- auf der *Registerkarte Banken* der entsprechenden Bank zugeordnet haben (s. Kapitel 7.1.1)
Entsprechende Zuordnungen müssen Sie auch in den verwendeten Zahlungsverkehrsmodulen vornehmen.



Beispiel: Erstzugangsbrief HBCI

```
                                                                        Köln, den 23.10.2003

       E R S T Z U G A N G S B R I E F


Frau
Monika Mustermann
In der Lohn 43

12345 Musterstadt




OMIKRON HBCI-Testbank
Von-Hünefeld-Strasse 55
50829 Köln

Telefon : 0221 / 59 56 99 - 0
Telefax : 0221 / 59 56 99 - 7



Sehr geehrte Kundin, sehr geehrter Kunde,

für das Einrichten eines neuen HBCI-Zugangs benötigten Sie folgende
Informationen

Benutzerkennung                 UMCC0001
Kunden-ID                       KMCC0001
Port für Verbindungsaufnahme:   3000
Internet-Adresse                123.456.789.012

Beiliegend erhalten Sie den INI-Brief über den öffentlichen Schlüssel
der Bank für die elektronische Signatur.

Nach erfolgreicher Initialisierung senden Sie bitte Ihren INI-Brief unterschrieben an die oben
aufgeführte Adresse, damit wir Ihren HBCI-Zugang freischalten können.

Diese Mitteilung wird nicht unterschrieben.
```



<u>Beispiel:</u> INI-Brief der Bank

```
Bank:




Schlüsselversion              0
Schlüsselnummer               1
HBCI-Version                  derzeit 2.01/2.10/2.20

Öffentlicher Schlüssel für die elektronische Signatur:

Exponent                       0768
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01

Modulus                        0768
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1B D1 9E 2F 70 30 70 9D 9E A1 66 99 57 A9 70 82
07 2A 65 D7 BC 34 6E 94 23 BC B5 61 A3 EB 00 63
E5 D3 9C 3D 2D E4 C8 41 CF 0D 5C BC 49 1B C9 8A
8B 00 5B DD 02 66 CF 06 20 28 37 BE BA 47 E1 17
1E 13 1F E5 5B 70 7E 9C 5A ED 56 9C DA A1 D0 7A
F1 FD 02 40 10 FD 74 A5 00 30 57 62 80 EC CC E7

Hash
3A F3 85 0F BE 83 AD 76 2A E5
B7 4E 3B 71 2D 1E 8A D9 D2 24
```



3.7 HBCI+

Für die Kommunikation per **HBCI+** (=HBCI mit PIN/TAN-Erweiterung) werden ebenfalls Bankparameterdateien benötigt. Die Bankparameterdateien werden dabei von Ihnen erstellt; die notwendigen Angaben erhalten Sie über die Institute, die diesen Kommunikationsweg anbieten. Dieses flexible Verfahren, das ohne weitere Installationen auskommt (wie Chipkartenleser und entsprechende Treiber-Software), verbindet die Sicherheit eines Einmalpasswortes (TAN) mit der in SSL bewährten 128 Bit-Transportverschlüsselung Ihres Browsers.

Sollten Sie das HBCI+-Verfahren nutzen wollen, müssen Sie zunächst sicherstellen, dass

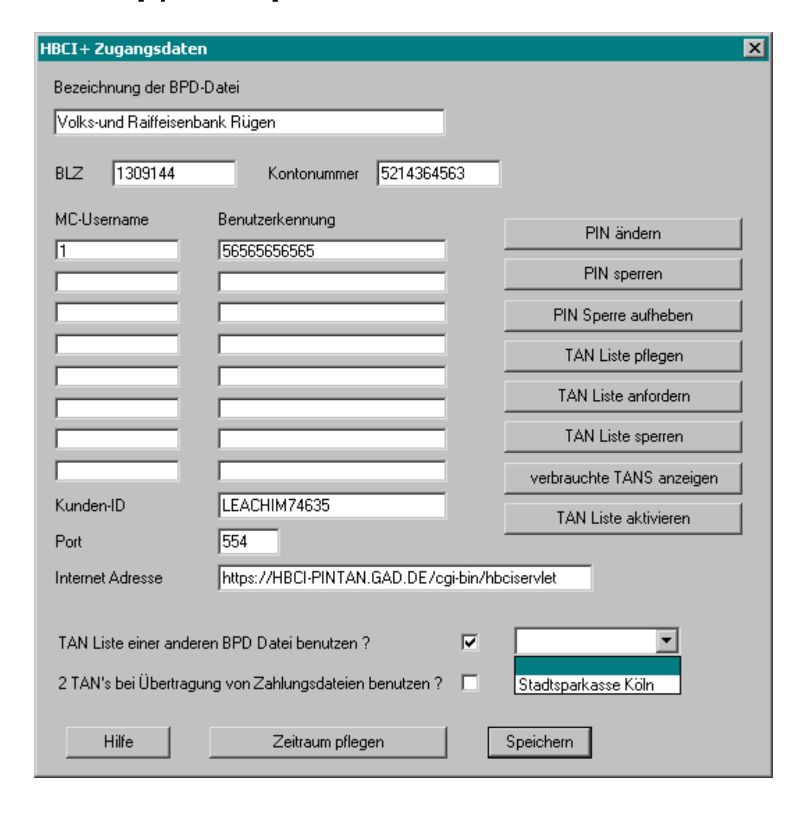
- bei der Installation das "Kommunikationsmodul HBCIPlus" installiert wurde,
- über den Menüpunkt -Kommunikation- / -DFÜ-Parameter- auf der *Registerkarte Prioritäten* das Verfahren "TCP/IP-Verbindung" angeklickt wurde. Auf der *Registerkarte TCP/IP-Verbindung* ist dann einzustellen, ob die Verbindung über ein DFÜ-Netzwerk oder LAN erfolgt.

Nach Drücken der Schaltfläche [***Neue BPD***] unter -Kommunikation- /-Bankparameterdateien-, Auswahl des Verfahrens "HBCIPLUS" über die Auswahlliste und Eingabe eines Namens für die Bankparameterdatei öffnet sich ein Dialog zur Eingabe der Zugangsdaten.



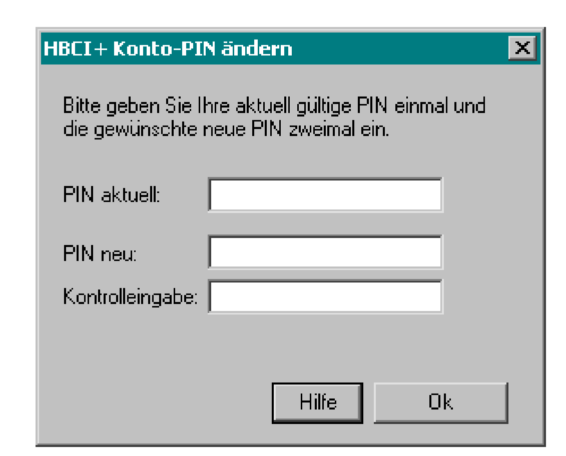
Der interne BPD-Dateiname darf maximal 8 Stellen haben und nur aus den Zeichen (A-Z,a-z,0-9,-,_) bestehen.

Die Ihnen mitgeteilten Daten tragen Sie analog zu HBCI in die Felder der folgenden Dialogbox ein und bestätigen anschließend mit [***Speichern***]:



In der Maske der HBCI+-Zugangsdaten können Sie über die Schaltfläche [***PIN ändern***] die PIN (= das Passwort) für Ihren HBCI+-Zugang ändern. Geben Sie dazu das neue Passwort in das entsprechende Feld ein. Im Feld Kontrolleingabe wiederholen Sie Ihre Eingabe zur Sicherheit noch einmal.

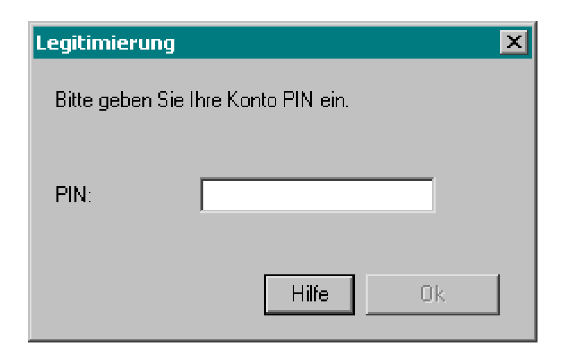




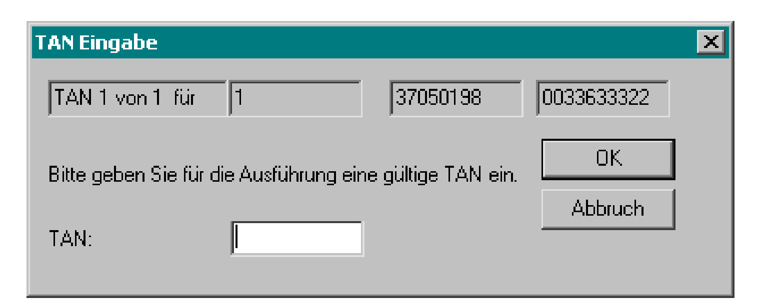
Bei Bedarf können Sie analog dazu in der Maske der HBCI+-Zugangsdaten über die entsprechenden Schaltflächen Ihre [***PIN sperren***] oder die [***PIN-Sperre aufheben***]. Weiterhin können Sie hier Ihre [***TAN-Liste pflegen***], eine neue [***TAN-Liste anfordern***] oder eine bestehende [***TAN-Liste sperren***]. Über die Schaltfläche [***Verbrauchte TANs anzeigen***] können Sie bereits verwendete TANs anzeigen lassen. Bei manchen Banken ist es notwendig, dass Sie Ihre TAN-Liste freischalten. Dies können Sie über die Schaltfläche [***TAN-Liste aktivieren***].

Ihre vom jeweiligen Kreditinstitut zur Verfügung gestellte TAN-Liste zu dem betreffenden Konto können Sie über die Schaltfläche [***TAN-Liste pflegen***] hinterlegen. Bei mehreren Benutzern kann der gerade eingeloggte Benutzer jeweils seine eigene TAN-Liste bearbeiten. Näheres dazu erfahren Sie in Kapitel 3.7.2: *TAN-Liste pflegen*.

Nach Drücken der genannten Schaltflächen müssen Sie sich zunächst durch Eingabe Ihrer Konto-PIN (= ihres Zugangs-Passwortes) legitimieren.

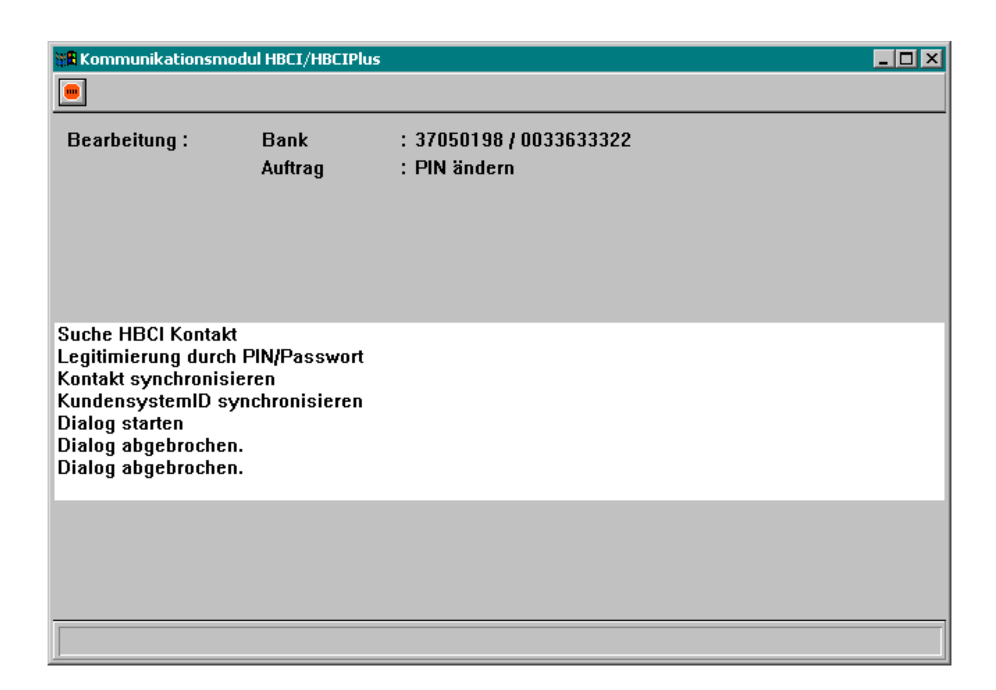


Einige der Aktionen wie das Ändern der PIN müssen Sie durch Eingabe einer TAN autorisieren. Geben Sie dazu eine gültige TAN in das entsprechende Feld ein und bestätigen Sie anschließend mit [***OK***].



Ergebnisse der Aktionen werden jeweils in einem Meldungsfenster bei der Kommunikation angezeigt, z. B.:





Ist eine Aktion nicht erfolgreich oder wird die entsprechende Funktion bankseitig nicht unterstützt, werden entsprechende Fehlermeldungen angezeigt.



Zusätzlich gibt es bei HBCI+ folgende Möglichkeiten:

TAN-Liste einer anderen BPD-Datei benutzen?

Wurde Ihnen für mehrere Konten eines Kreditinstituts nur **eine** TAN-Liste übergeben und ist die TAN-Liste bei einem anderen als dem aktuellen Konto, für das Sie die Zugangsdaten festlegen wollen, hinterlegt, markieren Sie das Kontrollkästchen entsprechend.

Aus der Auswahlliste hinter dem Kontrollkästchen wählen Sie anhand der ”sprechenden Bezeichnung” die Bank aus, für die bereits eine TAN-Liste hinterlegt ist, die auch vom aktuellen Konto mitbenutzt werden soll.

2 TANs zur Übertragung von Zahlungsaufträgen benutzen?

Wenn Sie das entsprechende Kontrollkästchen markieren, wird die Übertragung von Zahlungsaufträgen durch Eingabe einer zweiten TAN abgesichert. Der Zugriff auf die zweite TAN ist an einen zweiten Benutzer (mit einer zweiten PIN) gebunden. Dies bedeutet, dass in der Benutzerverwaltung mindestens zwei Benutzer eingetragen sind, die auch über die Berechtigung verfügen, einen Zahlungsauftrag zu versenden.
In der obigen Maske muss dann die linke Spalte "MC-Username" mit dem in der Benutzerverwaltung hinterlegten Benutzernamen des 2. Benutzers und die "Benutzerkennung" in der rechten Spalte ergänzt werden. (Die Benutzerkennung für den 2. Benutzer ist in der Regel identisch mit der Benutzerkennung des 1. Benutzers.) Schließlich werden die Angaben mit [***OK***] im Programmsystem gespeichert.

Jeder der Benutzer muss seine eigenen TANs hinterlegen, sofern er die TANs bei einer Übertragung nicht manuell eingeben will.

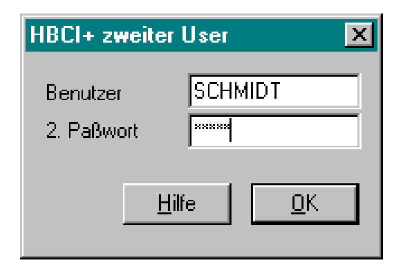


Jeder Benutzer erhält nur Zugang zu seinen eigenen TANs, d. h. der in obigem Beispiel eingetragene Benutzer "1" erhält beim Anklicken der Schaltfläche [***TAN-Liste pflegen***] nur seine eigenen TANs angezeigt. Der Benutzer "2" erhält erst dann Zugang zu seinen TANs, wenn er sich entsprechend anmeldet und dann die Schaltfläche [***TAN-Liste pflegen***] aufruft.

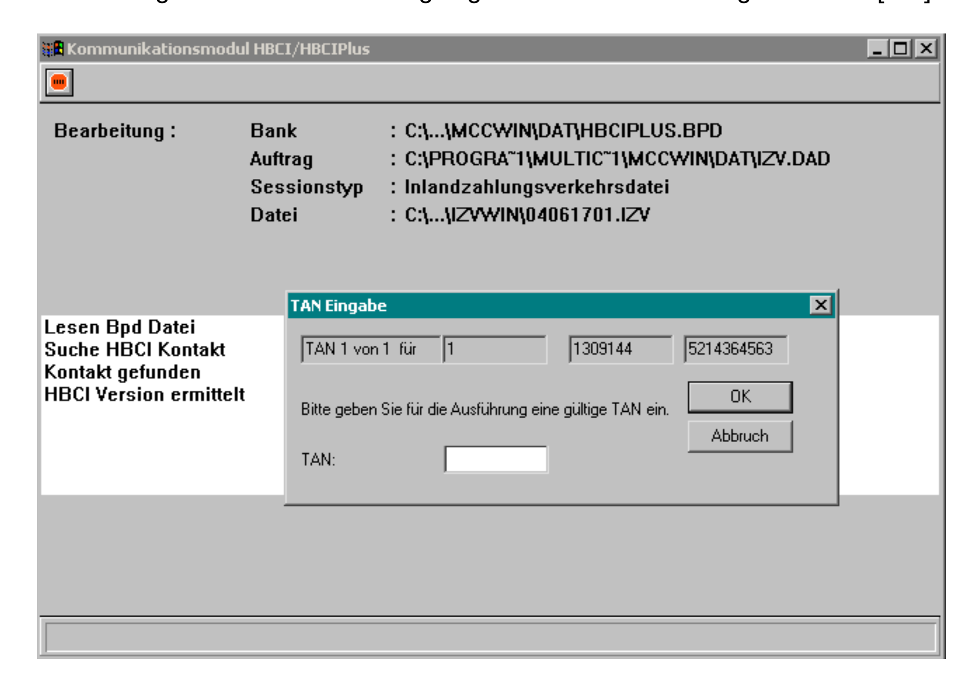
Wie wird eine Zahlung bei Absicherung durch eine zweite TAN verschickt?

Für den 1. Benutzer ändert sich nichts, d. h. er wird nach dem Versenden z. B. durch Anklicken der Schaltfläche [***Datei versenden***] im Dateimanager nach seiner PIN (und, falls nicht hinterlegt, auch nach seiner TAN) gefragt.

Sobald der 1. Benutzer die Eingabe seiner PIN mit [***OK***] bestätigt hat, geht ein weiteres Dialogfenster auf und der 2. Benutzer wird aufgefordert, sich mit seinem Benutzernamen anzumelden und seine PIN einzutragen.



Sofern für jeden der Benutzer die TAN-Liste gefüllt ist und noch eine genügende Anzahl an TANs enthält, erfolgt keine Abfrage nach manueller TAN-Eingabe. Sind beide oder auch nur eine TAN-Liste nicht ausreichend gefüllt, erscheint das benutzerabhängige Fenster zu manuellen TAN-Eingabe. Geben Sie eine gültige TAN ein und bestätigen Sie mit [***OK***].



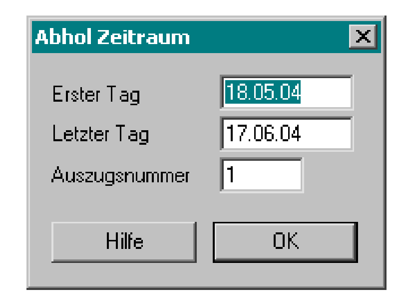
Erst wenn alle Voraussetzungen erfüllt sind, werden die Zahlungsaufträge verschickt.

Über die Schaltfläche [***Zeitraum pflegen***] können Sie analog zu HBCI (vgl. Kapitel 3.7.1*: Zeitraum pflegen*) den Abholzeitraum sowie die "Start"-Auszugsnummer von Kontoauszügen bei Bedarf abändern.



Eine "Zeitraum-Pflege" ist nur dann erforderlich, wenn Sie die vom Programmsystem vergebenen Standardeinstellungen verändern wollen.

Nach Aufruf der Schaltfläche [***Zeitraum pflegen***] erscheint eine Eingabemaske , in der das Feld "Erster Tag" das aktuelle Systemdatum - 1 Monat und das Feld "Letzter Tag" das aktuelle Systemdatum enthalten; das Feld "Auszugsnummer" ist mit 1 vorbelegt.



Sollen die Kontoinformationen zu einem anderen Anfangszeitpunkt und/ oder mit einer anderen "Start"-Auszugsnummer abgeholt werden, müssen Sie die Vorgabe entsprechend abändern.

Die Angabe eines Anfangszeitpunktes ist nur dann erforderlich, wenn Sie bisher noch keine Kontoinformationen bei Ihrer Bank abgeholt haben.

Im weiteren Programmverlauf wird das Datum im Feld "Letzter Tag" immer auf das aktuelle Systemdatum gesetzt. Im Feld "Erster Tag" wird immer das letzte Auszugsdatum + 1 Tag eingetragen. (Ausnahme: Beim letzten Abholvorgang wurde festgestellt, dass die abgeholten Kontoinformationen nicht vollständig sind. In diesem Fall lässt das Programm das Datum "Erster Tag" unverändert, damit beim nächsten Abholvorgang auch die noch fehlenden Daten übertragen werden können.)

Ist bereits ein Auszug für die in der BPD eingetragene Bankleitzahl mit der von Ihnen manuell eingetragenen Auszugsnummer in den Datenbanken des Cashmanagement-Moduls gespeichert, so wird dieser Auszug überschrieben. Achten Sie daher immer auf die korrekte Eingabe der "Start"-Auszugsnummer.

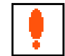
Im weiteren Programmbetrieb wird die Auszugsnummer nach jedem Abholvorgang um 1 erhöht. (Ausnahme: Beim letzten Abholvorgang wurde festgestellt, dass die abgeholten Kontoinformationen nicht vollständig sind. In diesem Fall lässt das Programm die Auszugsnummer unverändert, damit beim nächsten Abholvorgang auch die noch fehlenden Daten übertragen werden können.)

Schließlich bestätigen Sie Ihre Angaben in der Maske zu den $HBCI^{+}$-Zugangsdaten über die Schaltfläche [***Speichern***].

Um das Kommunikationsverfahren HBCI+ nutzen zu können, müssen Sie sicherstellen, dass Sie die erzeugte HBCI+-Bankparameterdatei unter -Hilfsdatenbanken- / -Banken- auf der *Registerkarte Banken* der entsprechenden Bank zugeordnet haben (s. Kapitel 7.1.1).
Entsprechende Zuordnungen müssen Sie auch in den verwendeten Zahlungsverkehrsmodulen vornehmen.



3.7.1 Zeitraum pflegen (HBCI und HBCI+)

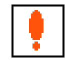


Eine "Zeitraum-Pflege" **ist nur dann erforderlich**, wenn Sie die vom Programmsystem vergebenen Standardeinstellungen verändern wollen.

Nach Aufruf der Schaltfläche [***Zeitraum pflegen***] erscheint eine Eingabemaske , in der die Felder die Felder "**Erster Tag**" und "**Letzter Tag**" das aktuelle Systemdatum enthalten; das Feld "Start-**Auszugsnummer**" ist mit 1 vorbelegt.

Sollen die Kontoinformationen zu einem anderen Anfangszeitpunkt und/ oder mit einer anderen Start-Auszugsnummer abgeholt werden, müssen Sie die Vorgabe entsprechend abändern.

Die Angabe eines Anfangszeitpunktes ist nur dann erforderlich, wenn Sie bisher noch keine Kontoinformationen über T-Online bei Ihrer Bank abgeholt haben.
Im weiteren Programmverlauf wird das Datum im Feld "Letzter Tag" immer auf das aktuelle Systemdatum gesetzt. Im Feld "Erster Tag" wird immer das letzte Auszugsdatum + 1 Tag eingetragen. (Ausnahme: Beim letzten Abholvorgang wurde festgestellt, dass die abgeholten Kontoinformationen nicht vollständig sind. In diesem Fall lässt das Programm das Datum "Erster Tag" unverändert, damit beim nächsten Abholvorgang auch die noch fehlenden Daten übertragen werden können.)



Ist bereits ein Auszug für die in der BPD eingetragene Bankleitzahl mit der von Ihnen manuell eingetragenen Auszugsnummer in den Datenbanken des Cashmanagement-Moduls gespeichert, so wird dieser Auszug überschrieben. Achten Sie daher immer auf die **korrekte Eingabe der Start-Auszugsnummer**.

Im weiteren Programmbetrieb wird die Auszugsnummer nach jedem Abholvorgang um 1 erhöht.

(Ausnahme: Beim letzten Abholvorgang wurde festgestellt, dass die abgeholten Kontoinformationen nicht vollständig sind. In diesem Fall lässt das Programm die Auszugsnummer unverändert, damit beim nächsten Abholvorgang auch die noch fehlenden Daten übertragen werden können.)

Sie übernehmen Ihre Einstellungen durch Betätigen der Schaltfläche [***OK***].



3.7.2 TAN-Liste pflegen (HBCI+)

Die Abkürzung "TAN" steht für **Transaktionsnummer**. Mit der Eingabe einer TAN schützen Sie Ihre Daten während der Übertragung vor unberechtigten Veränderungen und Eingriffen von aussen. Die TAN's stellen neben der PIN Ihre Zugangsberechtigung zum T-Online-Rechner dar. Bei jeder Übertragung von Zahlungsaufträgen wird eine TAN verbraucht. Zum Abholen von Kontoinformationen ist keine TAN erforderlich.

Sie erhalten von Ihrer Bank normalerweise 100 TANs per Post.
Die TANs sind jeweils einer bestimmten Bank und folglich einer bestimmten **Bankparameterdatei** zugeordnet.

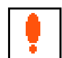
Sie können die Transaktionsnummern (TANs) auch in Ihrem System hinterlegen.
Nach Aufruf der Schaltfläche [***TAN-Liste pflegen***] öffnet sich eine kleine Maske zur Eingabe der PIN. Die zur BPD gehörende Tanliste kann nur geöffnet werden, wenn Sie die beim Anlegen der BPD vergebene PIN eintragen.

Anschließend betätigen Sie die Schaltfläche [***Tanliste***].

Bei der erstmaligen Pflege einer TAN-Liste steht Ihnen eine Tabelle zur Eingabe von maximal 100 TANs zur Verfügung.

Die Vergabe einer **Listennummer** ist nur bei einigen Rechenzentren erforderlich. In einem solchen Fall erhalten Sie eine entsprechende Nachricht von Ihrem Kreditinstitut.
Achten Sie bitte darauf, dass die TAN-Listennummer beim Rechenzentrum DVG Hannover (= Dialogart DVG) immer *7-stellig* ist.

Jede **TAN** besteht aus einer 6stelligen Ziffernkombination.



Achten Sie bitte auf korrekte Eingabe aller TANs, da eine Fehleingabe im weiteren Verlauf zum Abbruch des DFÜ-Auftrages führt.

Über die Schaltfläche [***Speichern***] speichern Sie die eingetragenen TANs ab. Sollte Ihnen Ihre Bank mehr als 100 TAN´s zugesandt haben, blättern Sie über [***Nächste Seite***] auf eine weitere Tabellenseite zur TAN-Eingabe.



3.8 ETEBAC3

Die meisten französischen Banken nutzen zur Datenübertragung das DFÜ-Verfahren ETEBAC3. Über ETEBAC3 können Zahlungsaufträge zur Bank geschickt und Kontoinformationen abgeholt werden.

Die für ETEBAC3 erforderliche BPD-Datei wird nach Auswahl des entsprechenden Menüpunktes editiert. Die zur Konfiguration der ETEBAC3-BPD benötigten Angaben werden Ihnen von Ihrer französischen Bank mitgeteilt.

Der Datenaustausch mit ETEBAC3 ist nur dann möglich, wenn Sie das entsprechende Zusatzmodul ETEBAC3 installiert haben.

Weitere Informationen finden Sie unter

- Erstellen einer ETEBAC3-BPD-Datei
- Einstellen von ETEBAC3-Parameterkarten

☞ **Beachten Sie bitte:**

Die zur Erstellung einer ETEBAC3-BPD erforderlichen Daten werden Ihnen immer von Ihrer französischen Bank auf Anfrage (meistens per Fax) mitgeteilt. Sie sollten daher immer vor Erstellung einer ETEBAC3 BPD Kontakt mit einem Bankberater Ihrer französischen Bank aufnehmen.

Übrigens:

Die von der französischen Bank über ETEBAC3 abgeholten Kontoauszüge werden im Hauptverzeichnis ..\MCCWIN unter dem Namen der entsprechenden Sicherungsdatei (*.STA) zusätzlich noch im Originalformat mit der Endung *.AFB abgelegt.



Erstellen einer ETEBAC3-BPD-Datei

Für die Erstellung einer ETEBAC3-BPD-Datei sind die folgenden Felder auszufüllen:

Bezeichnung der BPD-Datei

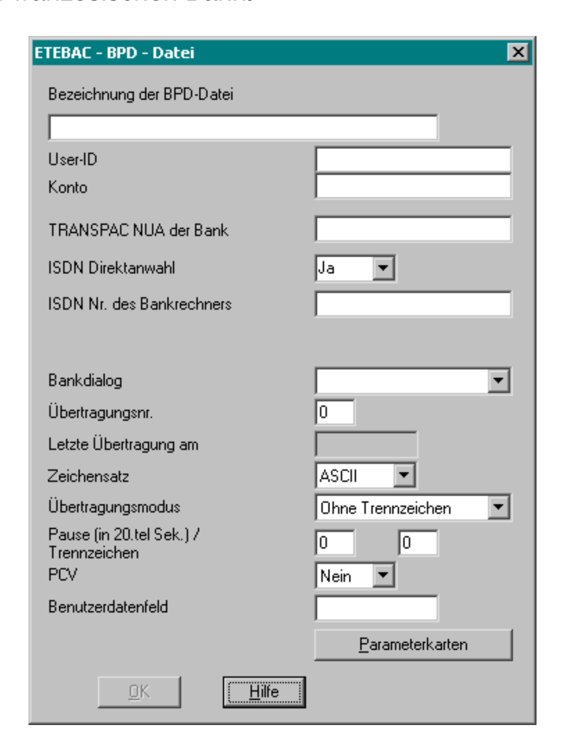
In dieses Feld tragen Sie eine aussagekräftige Bezeichnung der BPD ein. Im weiteren Programmverlauf wird diese Bezeichnung immer anstelle des Dateinamens der BPD verwendet.

User-ID

Dieses Feld dient zur Aufnahme der Kunden-ID, die zur Legitimation bei einigen Banken verwendet wird. Die User-ID erhalten Sie von Ihrer französischen Bank (immer in Großbuchstaben).

Konto

In dieses Feld tragen Sie Ihre Kontonummer bei der betreffenden Bank ein. Über die hier angegebene Kontonummer werden die per DFÜ übertragenen Zahlungsaufträge abgewickelt. Auch Abholaufträge von Kontoinformationen beziehen sich nur auf das angegebene Konto. In einigen Fällen wird anstelle der Kontonummer eine Zugangsnummer in dieses Feld eingetragen, die Ihnen für den Elektronischen Bankdienst zugeteilt wird. Nähere Informationen hierzu erhalten Sie von Ihrer französischen Bank.


ETEBAC - BPD - Datei

Bezeichnung der BPD-Datei

User-ID

Konto

TRANSPAC NUA der Bank

ISDN Direktanwahl: Ja

ISDN Nr. des Bankrechners

Bankdialog

Übertragungsnr.: 0

Letzte Übertragung am

Zeichensatz: ASCII

Übertragungsmodus: Ohne Trennzeichen

Pause (in 20.tel Sek.) / Trennzeichen: 0 / 0

PCV: Nein

Benutzerdatenfeld

Parameterkarten

OK

Hilfe

TRANSPAC-NUA der Bank

Über die hier einzutragende Transpac-Nummer (= NUA des Bankrechners) stellt das Programm die Verbindung zum Kommunikationsrechner Ihrer Bank her.

ISDN-Direktanwahl

Über dieses Listenfeld entscheiden Sie, ob es sich bei der Verbindung zu Ihrer Bank um eine ISDN-Direktverbindung handelt oder nicht. Wählen Sie "Ja", können Sie im nächsten Feld die "ISDN-Nummer der Bank" angeben. Ist "Nein" eingestellt, wird die indirekte Verbindung über einen französischen PAD gewählt und zwei andere Felder müssen gefüllt werden (siehe unten).

ISDN-Nummer der Bank

Wenn das Feld "ISDN-Direktanwahl" auf "Ja" gesetzt ist, erscheint dieses Feld, in das Sie die ISDN-Nummer der Bank für die Direktverbindung eintragen.



TRANSPAC ISDN-Nummer

Wenn das Feld "ISDN-Direktanwahl" auf "Nein" gesetzt ist, erscheint dieses Feld, wo Sie die ISDN-Nummer des französischen PAD (TRANSPAC: 08 36 08 64 64) eingeben.

NUA des Bankrechners (X25 B-Kanal)

Wenn das Feld "ISDN-Direktanwahl" auf "Nein" gesetzt ist, erscheint dieses zweite Feld, wo Sie die X25 NUA der Bank eintragen. Dies ist dieselbe Nummer wie im Feld "TRANSPAC-NUA der Bank".

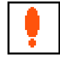
Bankdialog

Mit der Zusatzdiskette ETEBAC3 werden einsatzfähige Dialogdateien zur Kommunikation mit den französischen Banken ausgeliefert. Die zur Verfügung stehenden Dialoge sind in der Auswahlliste "Bankdialog" enthalten. Per Doppelklick wählen Sie den gewünschten Dialog aus der Liste aus.
(Der Dateiname besteht sich aus einem bis zu 8-stelligen Kürzel des entsprechenden Banknamens.)

Übertragungsnummer

Einige Banken schreiben vor, dass die einzelnen DFÜ-Sitzungen bezogen auf den jeweils aktuellen Tag mit einer fortlaufenden Nummer zu versehen sind. Beginnend mit der Nummer "0" wird dieser Wert nach jeder erfolgreichen Übetragung um 1 erhöht.

Verlangt Ihre Bank, dass eine DFÜ-Sitzung täglich mit einer bestimmten Übertragungsnummer zu beginnen hat, so tragen Sie hier den jeweiligen Startwert ein. Die Inkrementierung der Übertragungsnummer erfolgt im weiteren Programmverlauf automatisch. Allerdings müssen Sie nach einem Tageswechsel vor Durchführung eines DFÜ-Auftrages in solchen Fällen die Übertragungsnummer wieder auf den Startwert zurücksetzen.



Das Feld "Letzte Übertragung am" wird vom Programmsystem zu Ihrer Information mit dem Datum gefüllt, an dem die letzte erfolgreiche Übertragung unter Nutzung der entsprechenden BPD stattgefunden hat.

Letzte Übertragung am

Hier wird das Datum der letzten Übertragung angezeigt.

Zeichensatz

Über die Listbox wählen Sie den Zeichensatz, der bei der Datenübertragung genutzt werden soll.

Zur Auswahl stehen die Zeichensätze:

- EBCDIC (Voreinstellung)
- ASCII

Der Datenaustausch mit französischen Banken erfolgt in der Regel mit EBCDIC.

Übertragungsmodus

Über die Listbox wählen Sie, ob zwischen einzelnen Datensätzen jeweils die Zeichen "<CR><LF>" eingefügt werden sollen.

Zur Auswahl stehen die beiden Alternativen

- Mit Pause (kein <CR><LF>, Voreinstellung)
- Mit Trennzeichen (<CR><LF>)

Der Datenaustausch mit französischen Banken erfolgt in der Regel ohne <CR><LF>.



Pause nach Übertragung

Bankindividuell können Pausenzeiten zwischen einzelnen DFÜ-Sitzungen festgelegt werden. Die einzutragende Zahl bezieht sich auf eine Pause in 20stel Sekunden (Beispiel: ein Eintrag von "5" bedeutet eine Pause von 5/20 = 0,25 Sekunden).

Voreingestellt ist eine Pause von 5/20 Sekunden.

PCV

Dieses Feld gilt nur für X.25-Kommunikation und nur für die Kommunikation innerhalb Frankreichs: Kosten für die Kommunikation können durch die Bank getragen werden. Dazu ist der Parameter über das Listenfeld auf "Ja" zu setzen.

Benutzerdatenfeld

Hier steht für Ihre eigenen Zwecke eine Eingabemöglichkeit von bis zu 12 alphanumerischen Zeichen zur Verfügung.

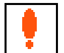
Über die Schaltfläche [***Parameterkarten***] legen Sie - sofern erforderlich - die speziellen Daten für die Datenübertragung fest.

Wenn Sie für den Datenaustausch mit einer Bank im Feld "Bankdialog" einen bestehenden Eintrag bereits gefunden und eingestellt haben, sind in der Regel in den Parameterkarten keine Veränderungen mehr notwendig. Änderungen an Parameterkarten sind nur auf Anweisung Ihrer Bank oder bei Konfiguration einer neuen Bank über den Bankdialog vorzunehmen

Sie übernehmen die Eintragungen durch Betätigen der Schaltfläche [***Speichern***].

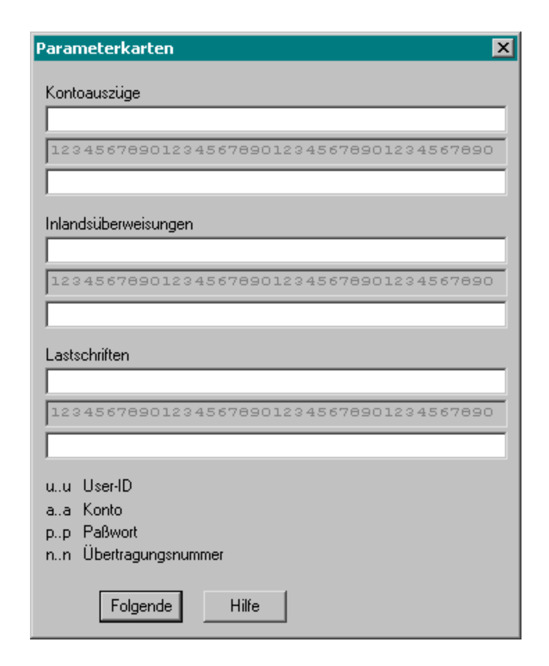


Einstellen von Parameterkarten



Die mit jeder Dialogart ausgelieferten Parameterkarten enthalten gültige Einstellungen. Eine Änderung ist deshalb nur unter bestimmten Umständen und in Ausnahmefällen erforderlich.

Parameterkarten sind Beschreibungen zur Kommunikation zwischen Bank- und Kundensystem für die verschiedenen Auftragsarten (z. B. Überweisungen, Lastschriften usw.). Eine Parameterkarte umfasst genau 80 alphanumerische Zeichen, die nach Vorgabe durch Ihre Bank belegt sein müssen. Wichtig ist dabei, dass die Eintragungen genau an den vorgegebenen Stellen erfolgen, also z. B. exakt an der Position 11 oder 22 oder 65.



Zur Verbesserung der Übersichtlichkeit wurde die Parameterbeschreibung auf 3 Zeilen aufgeteilt, wobei die erste und die dritte Zeile als Eingabezeile für maximal 40 Zeichen zur Verfügung stehen. Die mittlere Zeile hilft Ihnen bei der exakten Positionierung der einzutragenden Werte. In die erste Zeile tragen Sie bitte unter Beachtung der Positionierung die erforderlichen Werte für die Stellen 1 bis 40; in die dritte Zeile die Daten für die Stellen 41 bis 80 ein.

Sie haben die Möglichkeit, in den jeweiligen Parameterkarten

- User-ID
- Kontonummer
- Passwort
- Nr. der Übertragung

durch Variablen zu belegen. Welche Variable für welche Funktion in Frage kommt, ist in der letzten Maskenzeile erläutert. Zur Zeit kann

User-ID	durch	uuu ... uu
Kontonummer		aaa ... aa
Passwort		ppp ... pp
Nummer der Übertragung		nnn ... nn

bestimmt werden.

Sind die entsprechenden Bereiche der Parameterkarten mit Variablen ausgefüllt, so werden bei einer Datenübertragung an diese Stellen die in der ersten Bildschirmmaske zur Erstellung von ETEBAC3-BPDs vorgenommenen Einträge automatisch übernommen.



 **Beachten Sie bitte:**

Eine Ausnahme bildet die Variable "**p**" zur Bestimmung des DFÜ-Passwortes. Diese Variable muss **immer** in der Parameterkarte entsprechend der Vorgaben Ihrer Bank eingetragen werden. Die Variable wird dann während der DFÜ-Sitzung mit dem von Ihnen einzugebenden Passwort gefüllt.

In der aktuellen Programmversion können Parameterkarten bestimmt werden für:

- Kontoauszüge
- Inlandsüberweisungen
- Lastschriften
- LCR Inkasso senden
- Internationale Zahlungen
- Protokolldatei abholen
- Beliebige Datei senden
- Beliebige Datei abholen
- Rückläufer abholen
- LCR Auszug abholen
- Antwort auf LCR Auszug senden
- VSOT senden
- Clearing Avise abholen

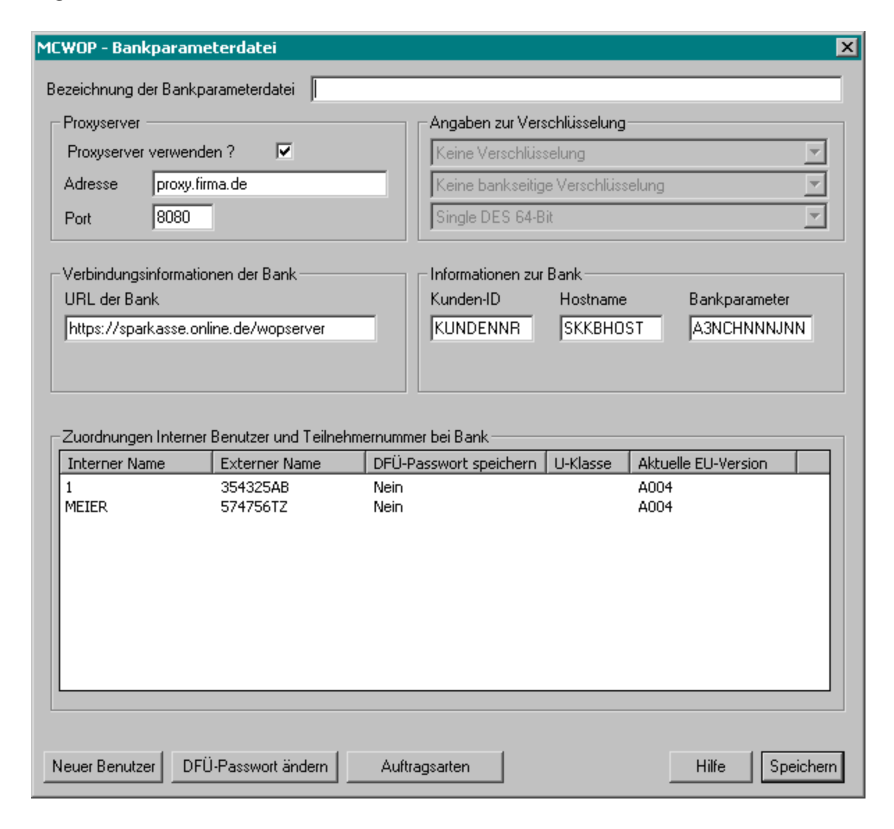
Die weiteren Parameterkarten rufen Sie jeweils über die Schaltfläche [***Folgende***] auf, die sich auf der ersten Seite der Einstellungen zu den Parameterkarten bzw. unten auf den einzelnen Parameterkarten befindet.
Auf der letzten Parameterkarte schließen Sie den Durchlauf über [***OK***] ab.



3.9 WOP

WOP (**W**eb **O**ngum **P**ortal) ist ein im Bereich der Sparkassen eingesetztes Verfahren zur Übertragung von Dateien über das Internet.

Die erforderlichen Angaben zur Konfiguration der WOP-BPD werden Ihnen von Ihrer Sparkasse mitgeteilt. Eine Ausnahme stellt das Feld "**Bezeichnung der Bankparameterdatei**" dar, in das Sie eine aussagekräftige Bezeichnung der BPD eintragen können. Im weiteren Programmverlauf wird diese Bezeichnung immer anstelle des Dateinamens der BPD verwendet.



Für die Anlage einer WOP-BPD stehen Ihnen die folgenden Felder zur Verfügung:

Proxyserver:

In der Regel erfolgt der Zugang ins Internet aus lokalen Firmennetzwerken heraus über einen Proxyserver. Soll ein vorhandener Proxyserver verwendet werden, markieren Sie das Kontrollkästchen "**Proxyserver verwenden?**".
Ist dieses Kontrollkästchen aktiviert, können Sie in die beiden nächsten Felder "**Adresse**" und "**Port**" die Adresse und die Portnummer des Proxyservers eintragen.

Angaben zur Verschlüsselung:

Unter "Angaben zur Verschlüsselung" finden Sie Angaben dazu, ob die kundenseitige oder die bankseitige Verschlüsselung in Betrieb genommen wurde.

Verbindungsinformationen der Bank:

Unter "**URL der Bank**" müssen Sie die Webadresse des Bankservers bzw. des Servers im zuständigen Rechenzentrum eintragen.



<u>Informationen zur Bank:</u>

Die bankseitig definierte **Kunden-ID** dient bei allen DFÜ-Aufträgen der Identifizierung des Kunden.
Den **Hostname**n und die **Bankparameter** bekommen Sie ebenfalls von Ihrer Bank mitgeteilt. Das Feld "Bankparameter" enthält eine Zeichenkette, bestehend aus einer Kombination von Buchstaben und Ziffern (vgl. Kapitel 3.3: *FTAM*).

<u>Zuordnungen Interner Benutzer und Teilnehmernummer bei der Bank:</u>

Die Zuordnungen von "**Interner Name**" (Benutzer im System) und "**Externer Name**" (Name bei der Bank) nehmen Sie wie für FTAM beschrieben vor. Ebenfalls können bis zu 512 Unterschriftsberechtigte in einer BPD gespeichert werden.

Über die Schaltfläche [***Neuer Benutzer***] bzw. den Kontextmenüeintrag -Neuaufnahme Benutzer- können neue Benutzer (aus dem am Rechner verfügbaren Benutzern) ausgewählt werden und in die BPD aufgenommen werden (neuer Datensatz wird angelegt). Durch Anklicken mit der linken Maustaste in der Auflistung bzw. über den Kontextmenüeintrag -Datensatz pflegen- (rechte Maustaste) können bestehende Datensätze editiert werden. Über -Löschen- und Bestätigen der Sicherheitsabfrage mit [***Ja***] können Benutzereinträge aus der BPD entfernt werden.

Zusätzlich kann für jeden Benutzer festgelegt werden, ob das DFÜ-Passwort in der Bankparameterdatei gespeichert werden soll. Dazu wählen Sie in der Spalte "**DFÜ-Passwort speichern**" aus der Liste entweder "Ja" oder "Nein".

In der Spalte "**U**(nterschrifts)**-Klasse** wird von der Bankseite diejenige Unterschriftsklasse eingetragen, die dort für den jeweiligen Teilnehmer definiert wurde.

In der Spalte "**Aktuelle EU-Version**" wird nach erfolgreicher Initialisierung die vom jeweiligen Teilnehmer verwendete EU-Version angezeigt.

Über die Schaltfläche [***DFÜ-Passwort ändern***] können Sie das Passwort, das in der BPD abgespeichert ist, ändern (vgl. *FTAM*).
Sie bestätigen anschließend Ihre Eingaben durch Anklicken von [***Speichern***].

Über die Schaltfläche [***Auftragsarten***] legen Sie fest, welche Auftragsarten zulässig sind bzw. ob eine Verschlüsselung möglich sein soll. Die Angaben werden zur Vorbelegung eines DFÜ-Auftrages herangezogen. Aus einer Auswahlliste der Auftragsarten suchen Sie die von Ihnen gewünschte Auftragart aus. Diese jeweils markierte Auftragsart bringen Sie durch Drücken der Schaltfläche [***Diese Auftragsart hinzufügen***] in die darunter befindliche Tabelle. In dieser Weise verfahren Sie solange, bis sich alle von Ihnen gewüschten Auftragsarten in der darunterliegenden Tabelle befinden. Anschließend können Sie für jede einzelne Auftragsart gesondert festlegen, ob eine Verschlüsselung erfolgen soll oder nicht soll und bestätigen schließlich mit [***Speichern***].

Durch Bestätigung über die Schaltfläche [***Speichern***] werden die Einstellungen schließlich in die Bankparameterdatei übernommen.



Inhaltsverzeichnis: Kapitel 4

Seite



4 Sonderfunktionen für die Kommunikation

Die Sonderfunktionen zu den DFÜ-Einstellungen beinhalten einige weniger häufig benötigte Funktionen für die Verwaltung Ihres DFÜ-Zugangs wie

- DFÜ-Passwort ändern
- Erstinitialisierung eines Bankzugangs
- Zurücksetzen eines ZVDFÜ-/MCFT-Zugangs
- Sperren eines DFÜ-Zugangs.

Die Möglichkeit zur

- Verschlüsselung

können Sie nutzen, wenn Sie die DFÜ-Verfahren FTAM bzw. FTP einsetzen.

Bei EBICS stehen neben einigen Funktionen, die im Rahmen der üblichen Assistenten abgewickelt werden (Erstinitialisierung, Sperrung), einige spezielle Funktionen in gesonderten Menüpunkten zur Verfügung:

- FTAM-/FTP-Bankzugang auf EBICS umstellen
- EBICS-Authentifikationsschlüssel austauschen
- EBICS-DFÜ-Passwort ändern

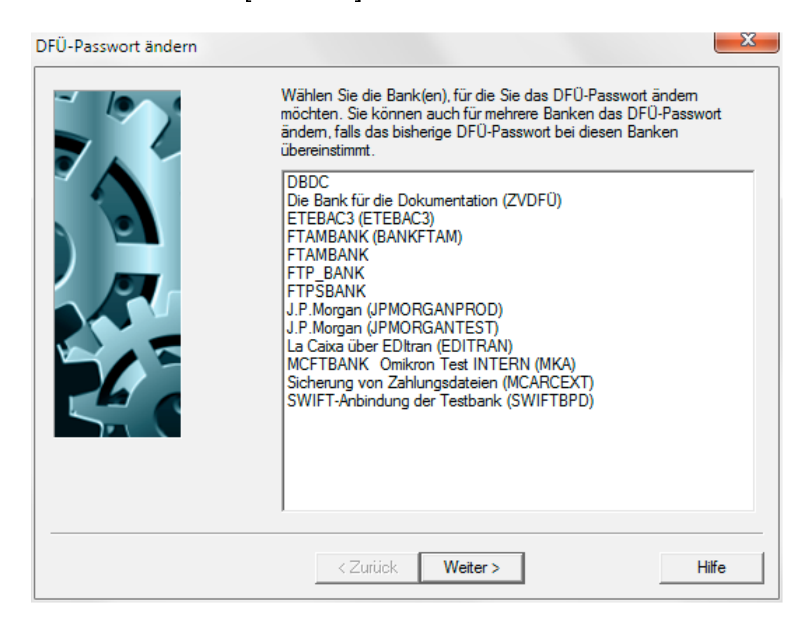


4.1 DFÜ-Passwort ändern (Sessiontyp PWA)

Um ein bestehendes DFÜ-Passwort zu ändern, wählen Sie im Menü -Kommunikation- den Menüpunkt - DFÜ-Passwort ändern-.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, wenn Sie Ihr DFÜ-Passwort ändern möchten:

1 **Auswahl der Bank(en)**
Die im System gespeicherten Banken, bei denen Sie das Passwort ändern können, werden Ihnen in einer Liste angeboten. Wählen Sie die Bank mittels Mausklick aus, für die Sie das DFÜ-Passwort ändern möchten. Sie können auch für mehrere Banken das DFÜ-Passwort ändern, falls z. B. das bisherige DFÜ-Passwort bei diesen Banken übereinstimmt. Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].



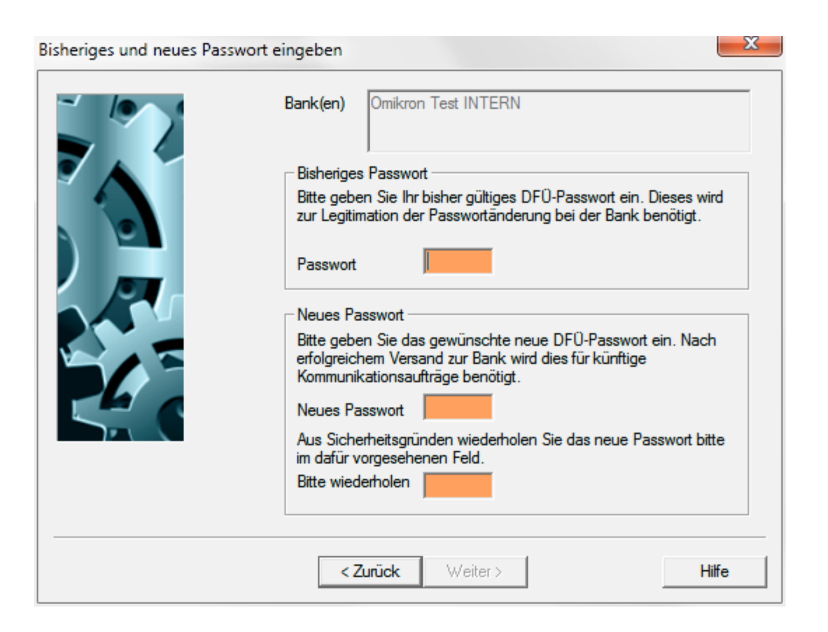
2 **Bisheriges und neues Passwort eingeben**
Unterhalb der ausgewählten Bank(en) erscheinen nun drei Pflichteingabefelder. Geben Sie zunächst unter "Bisheriges Passwort" Ihr bisher gültiges DFÜ-Passwort ein. Dieses wird zur Legitimation der Passwortänderung bei der Bank benötigt.
Wechseln Sie dann mit der TAB-Taste zum nächsten Eingabefeld und geben Sie dann unter "Neues Passwort" das gewünschte neue DFÜ-Passwort ein. Nach erfolgreichem Versand zur Bank wird dieses für künftige Kommunikationsaufträge benötigt.

Da die Passwortvergabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit im dafür vorgesehenen Feld wiederholen.

☞ **Beachten Sie bitte:**
Bei der Erfassung des Passwortes werden -abweichend von der sonst üblichen Praxis- die Eingaben **nicht** in Großbuchstaben umgesetzt. Es wird also zwischen Groß- und Kleinschreibung unterschieden. Dies ist bei der Erfassung und späteren Verwendung des Passwortes zu berücksichtigen.

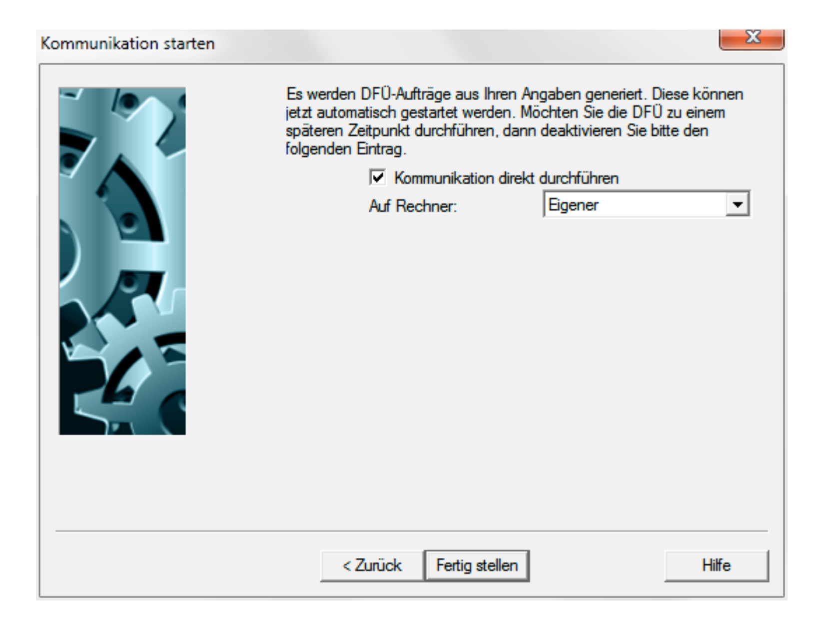
Sie schließen die Passworteingabe ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.





3 **Kommunikation starten**

Es wird eine DFÜ-Auftragsdatei aus Ihren Angaben generiert. Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**". Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.



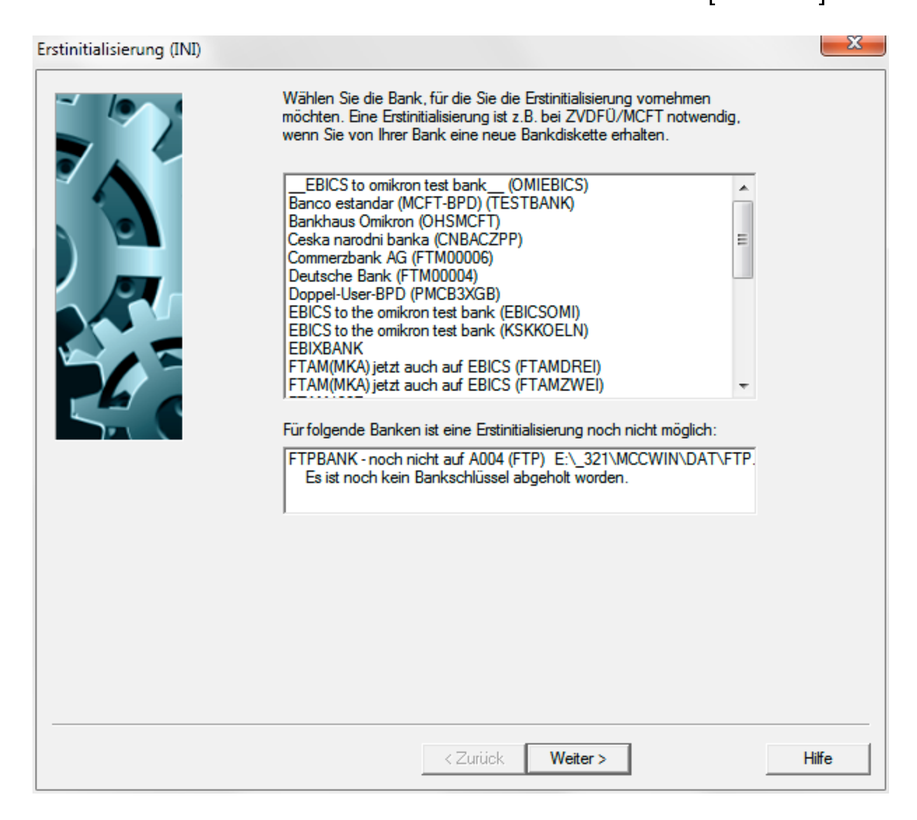
Über die Schaltfläche [**<** ***Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.

4.2 Erstinitialisierung eines Bankzugangs durchführen (Sessiontyp INI)

Um eine Erstinitialisierung durchzuführen, wählen Sie im Menü -Kommunikation- den Menüpunkt -Erstinitialisierung-. Eine Erstinitialisierung ist z. B. bei ZVDFÜ/MCFT notwendig, wenn Sie von Ihrer Bank eine neue Bankdiskette erhalten.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um die Erstinitialisierung durchzuführen. Zunächst werden Sie aufgefordert, die entsprechende Bankdiskette einzulegen.

1 **Auswahl der Bank(en)**
Wählen Sie die Bank(en) aus der Liste mittels Mausklick aus, für die Sie die Erstinitialisierung vornehmen möchten. Drücken Sie anschließend auf die Schaltfläche [***Weiter*** **>**].

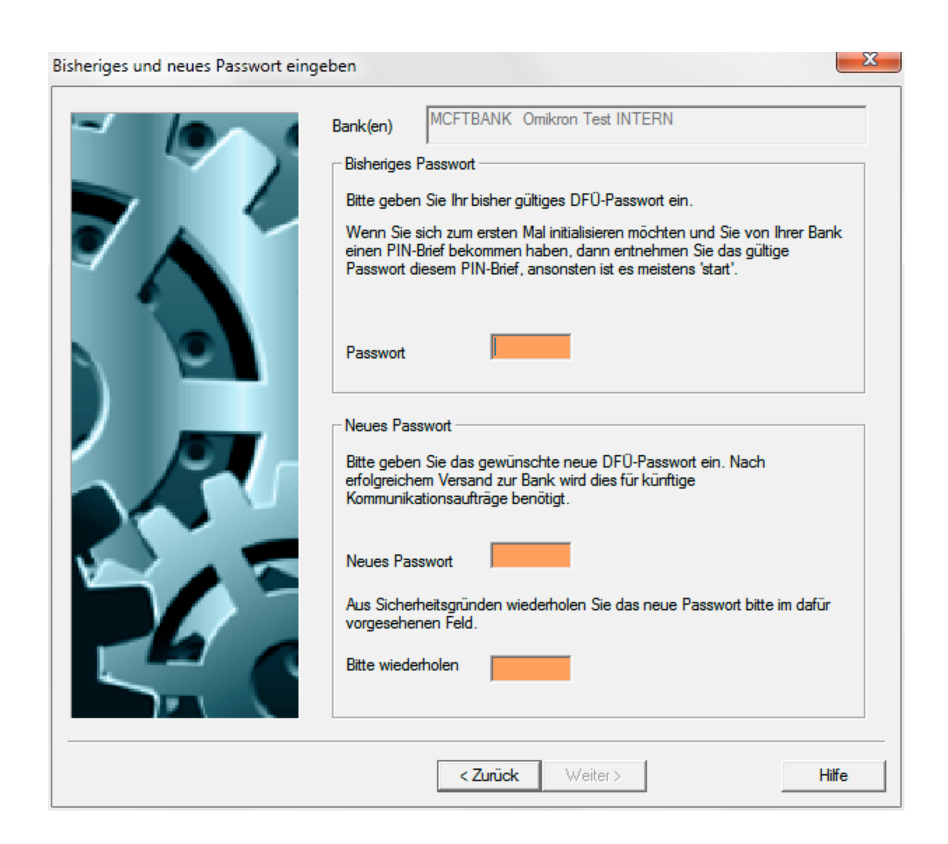


Banken, für die eine Erstinitialisierung noch nicht möglich ist, erscheinen in einer zweiten Liste zusammen mit einem Hinweistext zur Ursache, z. B. "Es ist noch kein Bankschlüssel abgeholt worden".

2 **Bisheriges und neues Passwort eingeben**
Unterhalb der ausgewählten Bank(en) erscheinen nun drei Pflichteingabefelder. Geben Sie zunächst unter "Bisheriges Passwort" Ihr bisher gültiges DFÜ-Passwort ein. Dieses wird zur Legitimation der Erstinitialisierung bei der Bank benötigt.
Wenn Sie von Ihrer Bank einen PIN-Brief bekommen haben, entnehmen Sie das gültige Passwort diesem PIN-Brief. Ansonsten ist das erste Passwort meistens "start".
Wechseln Sie dann mit der TAB-Taste zum nächsten Eingabefeld und geben Sie dann unter "Neues Passwort" das gewünschte neue DFÜ-Passwort ein. Nach erfolgreichem Versand zur Bank wird dieses für künftige Kommunikationsaufträge benötigt.

Da die Passwortvergabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit im dafür vorgesehenen Feld wiederholen. Ggf. muss ein zweites Passwort eingegeben werden und dessen Neueingabe ebenfalls wiederholt werden.

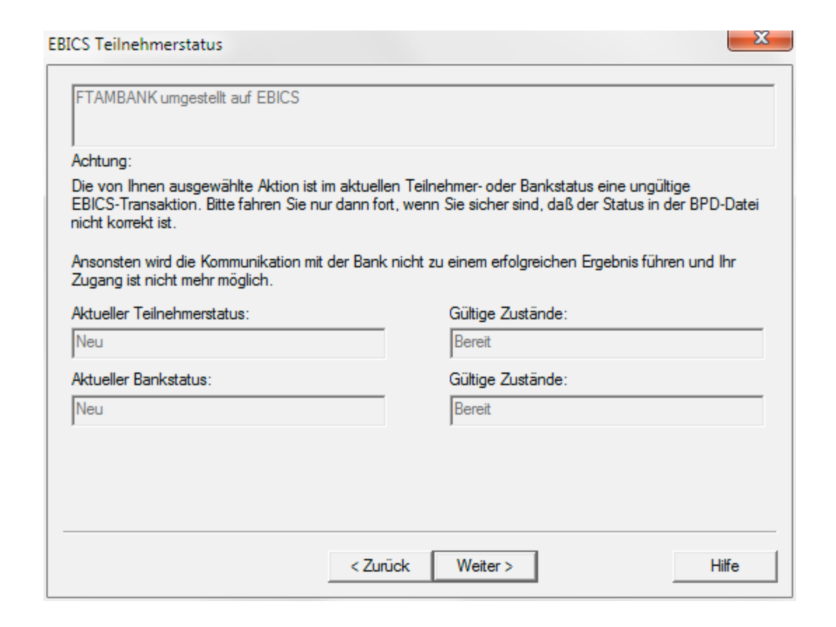




Beachten Sie bitte:

Bei der Erfassung des Passwortes werden -abweichend von der sonst üblichen Praxis- die Eingaben **nicht** in Großbuchstaben umgesetzt. Es wird also zwischen Groß- und Kleinschreibung unterschieden. Dies ist bei der Erfassung und späteren Verwendung des Passwortes zu berücksichtigen.

Sie schließen die Passworteingabe ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.



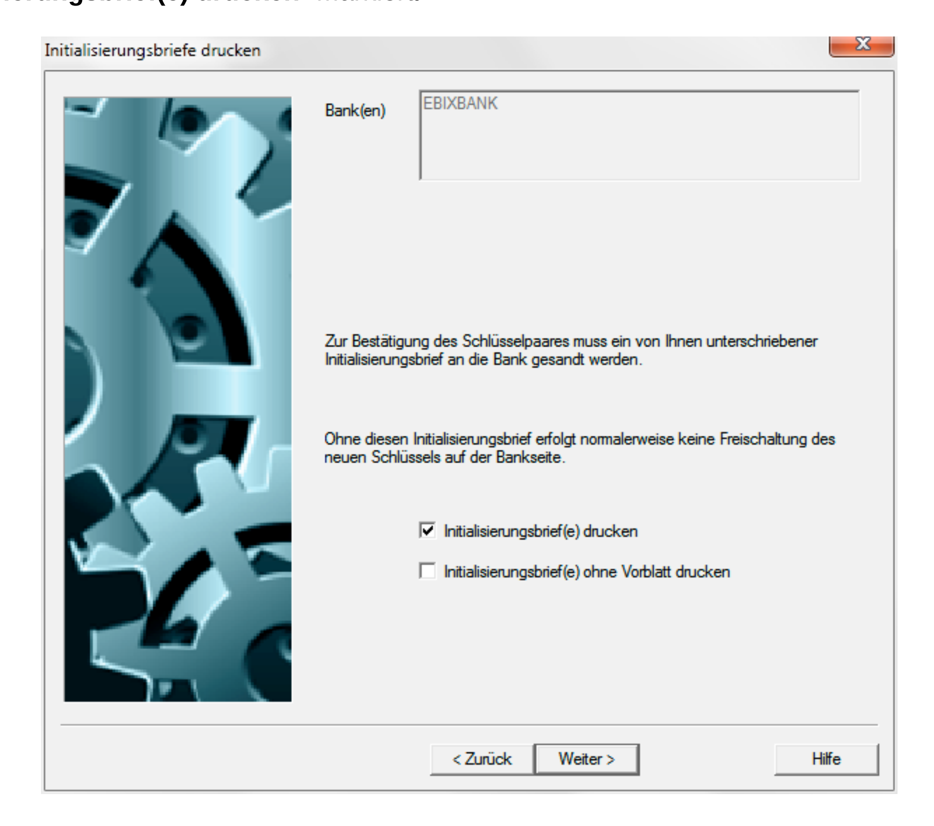
nur bei EBICS:

Ist der Teilnehmerstatus abweichend von "Neu" oder "Gesperrt", erscheint hier bei EBICS eine Warnmeldung. Ansonsten folgt direkt Punkt 3.



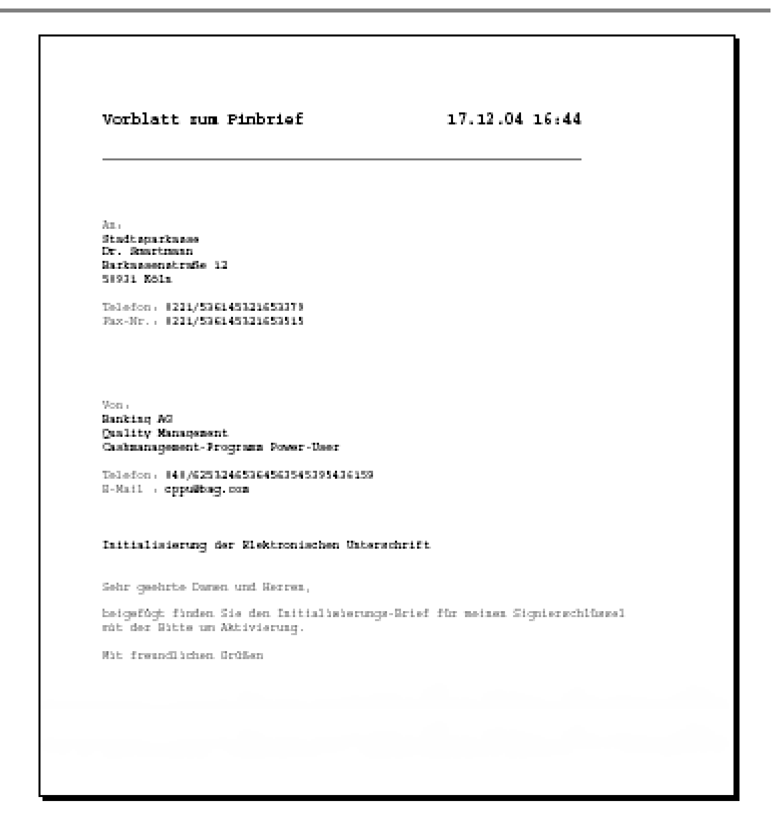
3 **Initialisierungsbriefe drucken**

Zur Bestätigung (eines bereits erstellten) Schlüsselpaares, muss ein von Ihnen unterschriebener Initialisierungsbrief an die Bank gesandt werden. Ohne diesen Initialisierungsbrief erfolgt normalerweise keine Freischaltung des neuen Schlüssels auf der Bankseite. Möchten Sie die den/die Initialisierungsbrief(e) ausdrucken, lassen Sie das Kontrollkästchen "**Initialisierungsbrief(e) drucken**" markiert.



Zusammen mit den INI-Formularen wird automatisch pro Bank ein Anschreiben erstellt, sofern eine Bankparameterdatei zugeordnet wurde. Die Adressdaten dafür werden den Eintragungen auf der *Registerkarte Banken*: Informationen zur Bank (s. Basismodul-Kapitel 7.1.1) und auf der *Registerkarte Kontakte* (s. Basismodul-Kapitel 5.4.4) entnommen.





Vorblatt zum Pinbrief 17.12.04 16:44

An:
Stadtsparkasse
Dr. Smartmann
Sparkassenstraße 12
50931 Köln

Telefon: 0221/5361453216533?9
Fax-Nr.: 0221/536145321653515

Von:
Banking AG
Quality Management
Cashmanagement-Programm Power-User

Telefon: 040/6251246536456254539543615?
E-Mail : cppu@bag.com

Initialisierung der Elektronischen Unterschrift

Sehr geehrte Damen und Herren,

beigefügt finden Sie den Initialisierungs-Brief für meinen Signierschlüssel mit der Bitte um Aktivierung.

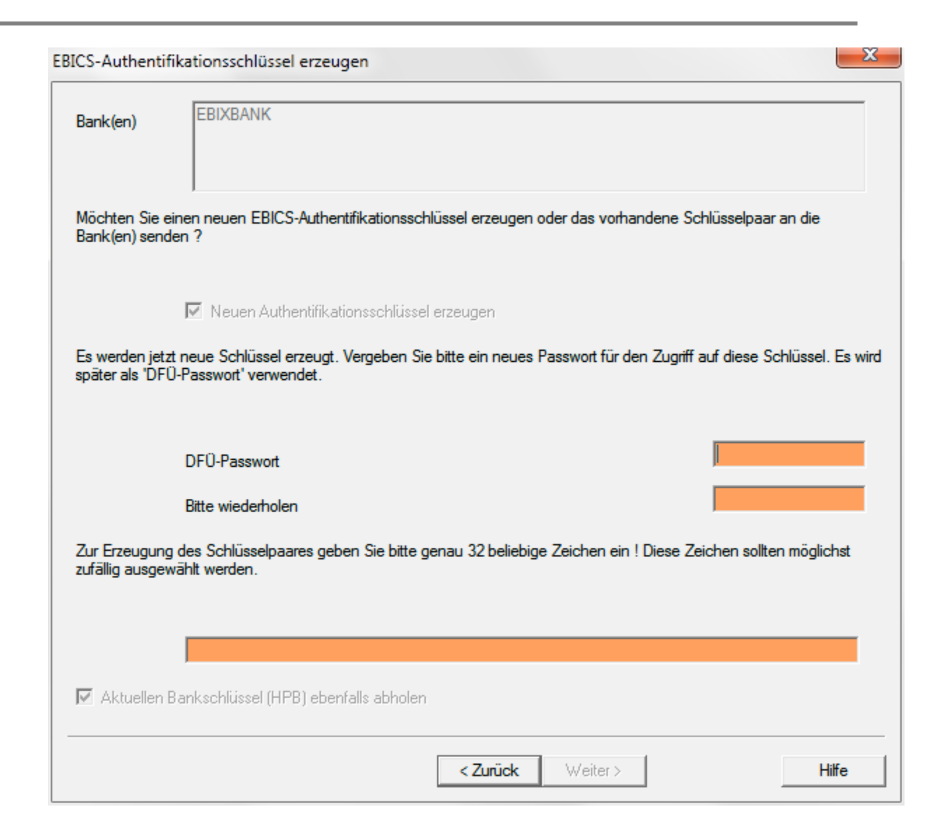
Mit freundlichen Grüßen

Wenn bei der Erstinitialisierung etlicher Benutzer bei einer Bank nicht jedesmal dieses "Vorblatt" gedruckt werden soll, können Sie die Generierung unterbinden, indem Sie zusätzlich das Kontrollkästchen "**Initialisierungsbrief(e) ohne Vorblatt drucken**" markieren.
Drücken Sie dann die Schaltfläche [***Weiter >***].

4 **Signaturschlüssel erzeugen**
Sofern noch kein Schlüsselpaar für die bankfachliche Signatur erzeugt wurde, wird anschließend zunächst der Assistent/Dialog zur Schlüsselpaar-Generierung bzw. für den Import der öffentlichen Schlüssel vom Signaturmedium gestartet (zu den Eingabefeldern s. Kapitel 6.1: *EU-Schlüsselpaar generieren / versenden*).

EBICS-Authentifikationsschlüssel erzeugen (nur bei EBICS)
Haben Sie noch keine A- und V-Schlüssel erzeugt, können Sie dies auf dieser Seite tun. Im Dialogfenster ist das Kontrollkästchen "**Neuen Authentifikationsschlüssel erzeugen**" bereits markiert. Möchten Sie ein neues Schlüsselpaar für die EBICS-Authentifikation generieren, belassen Sie diese Voreinstellung.





Sollen dagegen bereits vorhandene (z. B. bereits früher für eine andere Bank erzeugte) Schlüssel an die Bank(en) versandt werden, demarkieren Sie das Kontrollkästchen. Geben Sie in diesem Fall Ihr bereits gültiges DFÜ-Passwort ein.

Bei markierter Option werden anschließend neue Schlüssel erzeugt. Vergeben Sie bitte für den Zugriff auf die Schlüssel ein neues Passwort. Es wird später als "**DFÜ-Passwort**" verwendet. Da die Passworteingabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit im dafür vorgesehenen Feld **bitte wiederholen**.

Sofern Sie das Kontrollkästchen zur Schlüsselpaarerzeugung markiert haben, müssen Sie unterhalb des Feldes für die Passworteingabe eine beliebige Zeichenkette bestehend aus exakt **32 Zeichen** eingeben. Diese Zeichen sollten möglichst zufällig ausgewählt werden. Die Eingabe erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt. Diese frei wählbare Zeichenkette bildet die Basis zur Erstellung des Schlüsselpaares.

Über das Kontrollkästchen "**Aktuellen Bankschlüssel (HPB) ebenfalls abholen**" können die Bankschlüssel abgeholt werden. Dies ist nur notwendig, wenn für diese BPD noch keine Bankschlüssel vorliegen. Steht der Status der Bankschlüssel in der BPD auf "Bereit", wird das Kontrollkästchen zum Abholen der Bankschlüssel ohne Markierung vorbelegt und deaktiviert.

Drücken Sie abschließend auf die Schaltfläche [***Weiter >***].

 **Beachten Sie bitte:**

Haben Sie das Kontrollkästchen "**Neuen Authentifikationsschlüssel erzeugen**" markiert, obwohl bereits gültige Schlüssel existieren, erfolgt anschließend ein Warnhinweis.

Wenn Sie hier fortfahren, müssen Sie anschließend das neue Schlüsselpaar auch an Ihre bereits freigeschalteten EBICS-Banken senden, ansonsten können Sie mit diesen nicht mehr weiterarbeiten.

Sie können an dieser Stelle eine Seite zurückgehen und die Markierung des Kontrollkästchens ggf. zurücknehmen.

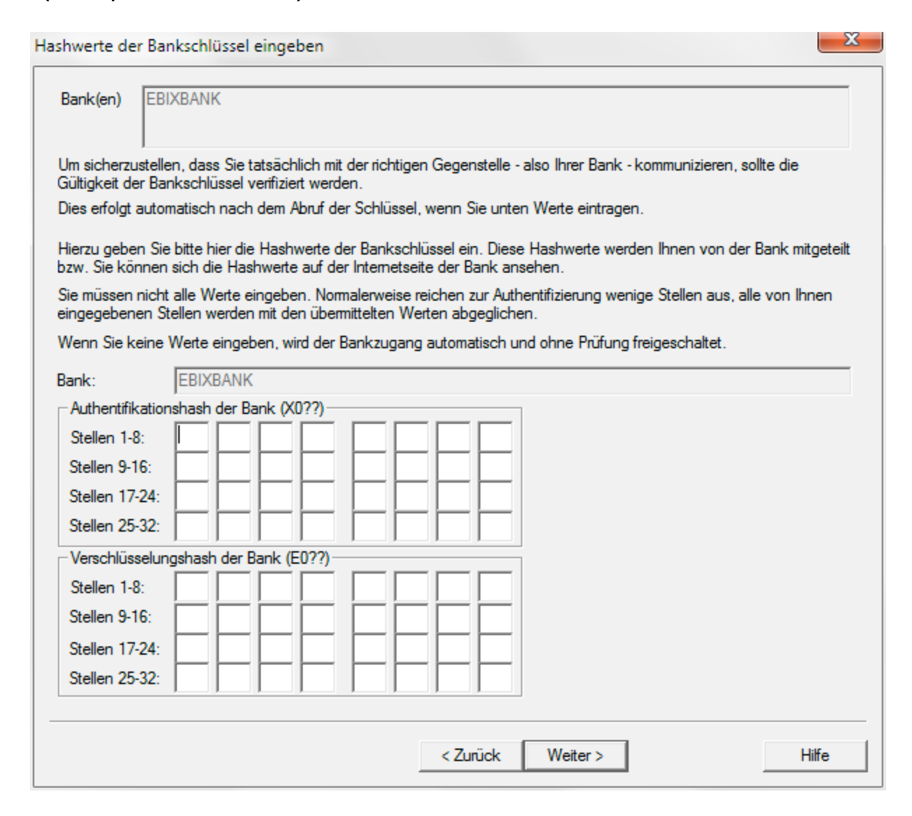


5 **Hashwerte der Bankschlüssel eingeben (nur bei EBICS)**
Um sicherzustellen, dass Sie tatsächlich mit der richtigen Gegenstelle -also Ihrer Bank- kommunizieren, sollte die Gültigkeit der Bankschlüssel, die am Ende dieses Assistenten abgeholt werden, verifiziert werden. Dies erfolgt automatisch nach Abruf der Schlüssel.

Geben Sie bitte dafür die Hashwerte der Bankschlüssel in die vorgesehenen Felder ein (**Authentifikationshash der Bank (X0??)** / **Verschlüsselungshash der Bank (E0??)**). Diese Hashwerte werden Ihnen von der Bank mitgeteilt bzw. Sie können sich die Hashwerte auf der Internetseite der Bank ansehen.

Sie müssen nicht alle Werte eingeben. Normalerweise reichen zur Authentifizierung wenige Stellen aus. Alle von Ihnen eingegebenen Werte werden mit den übermittelten Werten abgeglichen.
Die Werte im jeweils ersten Feld sind Pflicht, wenn sie von "00" abweichend sind.

Sie können den Status der Bankschlüssel im Menüpunkt -Kommunikation- / -Bankparameterdateien- in der Bankparameterdatei überprüfen und die Verifikation nachträglich durch Eingabe und Abspeichern der Hashwerte über die Schaltfläche [***Hashwerte der Bank***] wiederholen (s. Kapitel 3.5: *EBICS*).



Drücken Sie dann die Schaltfläche [***Weiter >***].

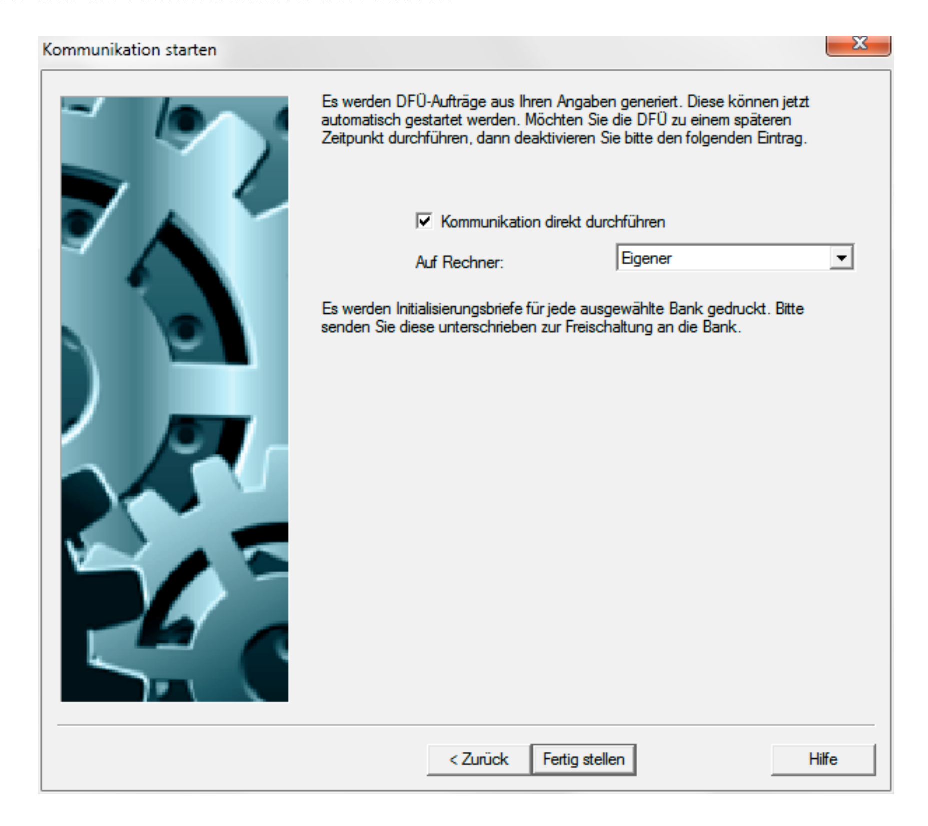
6 **Kommunikation starten**
Es wird ein Kommunikationsauftrag aus Ihren Angaben generiert.
Bei EBICS werden folgende Kommunikationsaufträge automatisch vom Assistenten erzeugt und in den Datei-Manager eingestellt:

INI,



HIA (Übermittlung der Public Keys des Benutzers für Authentifikation und Verschlüsselung) und HPB (Abholung der Bankschlüssel)

Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".
Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.



Über die Schaltfläche [***< Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.

Bei EBICS werden die Kommunikationsaufträge INI und HIA nach Drücken der Schaltfläche [***Fertig stellen***] sofort ausgeführt.

Die Bankschlüssel können erst abgeholt werden, wenn der Benutzer auf Bankseite freigeschaltet ist. Dabei werden die Hash-Werte der Bank nur einmal je BPD gehalten (also nicht je Teilnehmer) und automatisch abgeglichen und freigeschaltet, soweit sie bereits in der BPD hinterlegt waren.

Daher wird der HPB-Auftrag vom Assistenten mit dem Status "Wartet auf DFÜ" in den Dateimanager eingestellt (nur falls noch kein Bankschlüssel vorhanden ist), so dass er dort nach der Freischaltung einfach ausgeführt werden kann. Ein entsprechender Hinweis für den Benutzer wird eingeblendet:

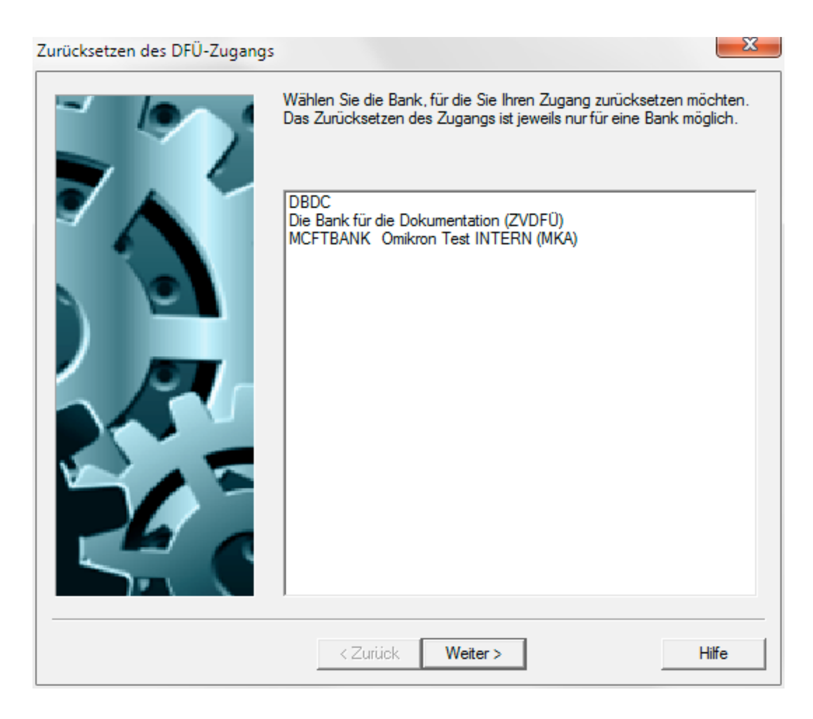


4.3 Zurücksetzen eines ZVDFÜ/MCFT-Zugangs (Sessiontyp RES)

Um einen Bankzugang zurückzusetzen, wählen Sie im Menü -Kommunikation- den Menüpunkt -Zurücksetzen eines ZVDFÜ/MCFT-Zugangs-.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um einen Bankzugang zurückzusetzen. Das Zurücksetzen ist jeweils nur für eine Bank möglich.

1 **Auswahl der Bank**
Wählen Sie die Bank aus der Liste mittels Mausklick aus, für die Sie ihren Zugang zurücksetzen möchten.



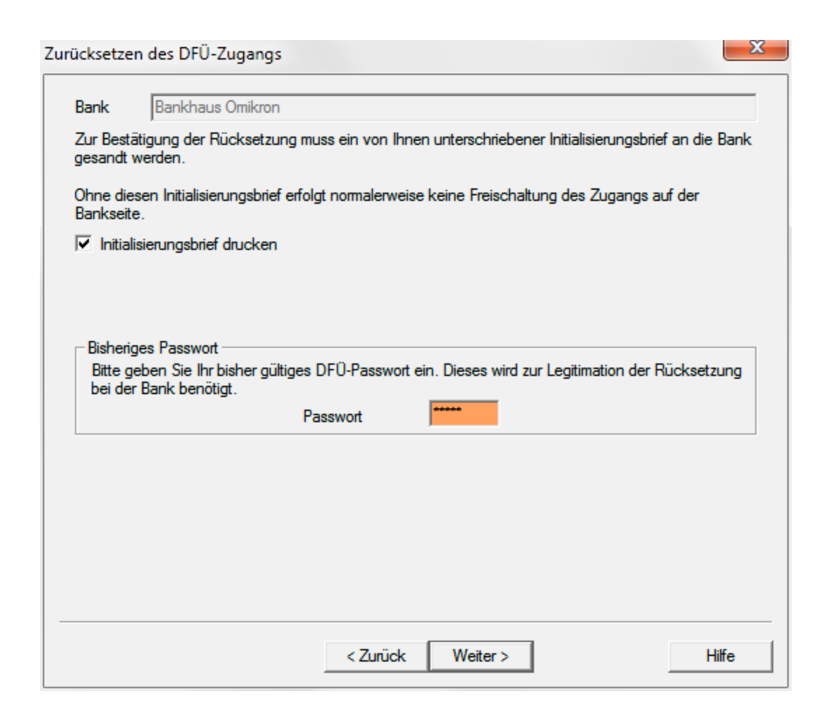
Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].

2 **Initialisierungsbrief drucken / Rücksetzung mittels Signatur**
Zur Bestätigung der Rücksetzung muss ein von Ihnen unterschriebener Initialisierungsbrief an die Bank gesandt werden. Ohne diesen Initialisierungsbrief erfolgt normalerweise keine Freischaltung des Zugangs auf der Bankseite. Lassen Sie daher das Optionsfeld "**Initialisierungsbrief drucken**" markiert.

Außerdem müssen Sie das bisher gültige DFÜ-**Passwort** eingeben. Es wird zur Legitimation der Rücksetzung bei der Bank benötigt.

Sie tragen das DFÜ-Passwort in das entsprechende Feld. Die Passwortvergabe erfolgt verdeckt, d. h. jeder Tastendruck wird durch ein * (Sternchen) dargestellt.

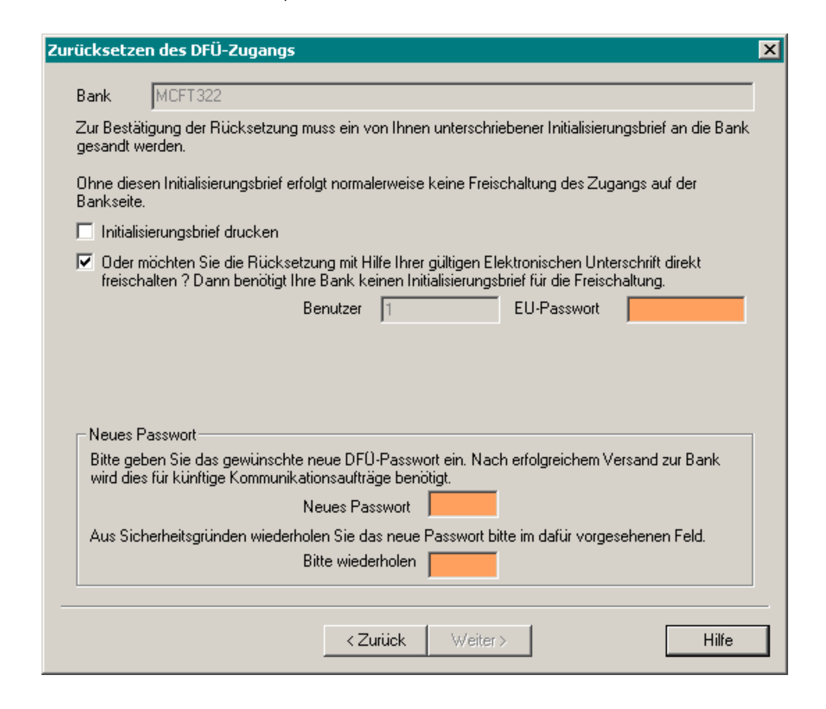




Sofern vom Banksystem unterstützt, kann die **Rücksetzung** auch **mittels Signatur** direkt freigeschaltet werden. Markieren Sie dazu die zweite Option. Geben Sie anschließend Ihr "**EU-Passwort**" ein.

Weiterhin müssen Sie das neue DFÜ-**Passwort** für Ihre künftigen Kommunikationsaufträge eingeben. Das Passwort muss zur Sicherheit **wiederholt** werden.

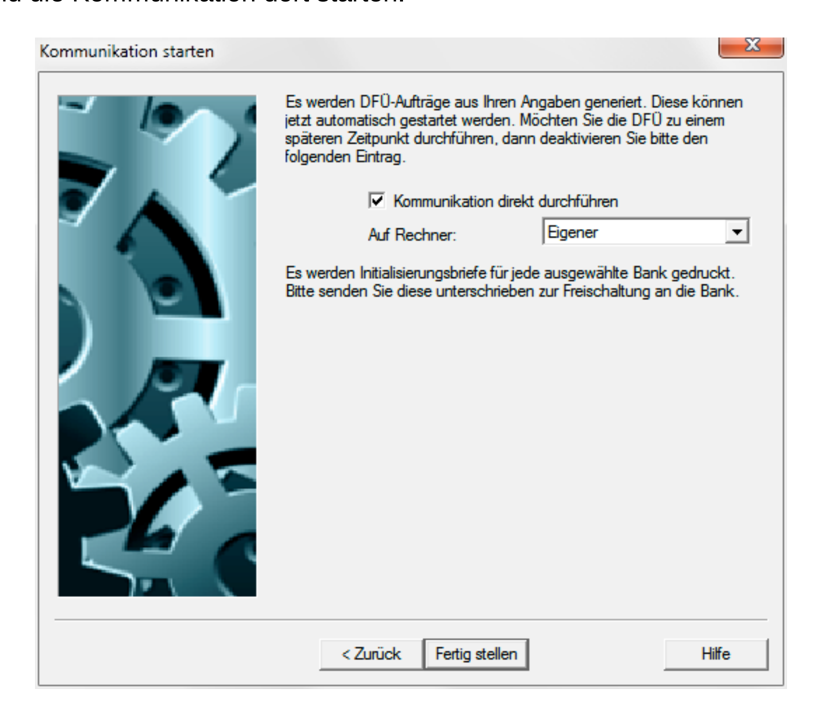
Kann die Unterschrift vom Banksystem verifiziert werden, sind die Schlüssel und das neue DFÜ-Passwort in einem Schritt aktualisiert, ohne dass ein Freischalten durch die Bank erfolgen muss.



Sie schließen diese Seite ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.



3 **Kommunikation starten**
Es wird eine DFÜ-Auftragsdatei aus Ihren Angaben generiert. Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".
Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.



Über die Schaltfläche [***< Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.

Anschließend werden Initialisierungsbriefe für jede ausgewählte Bank gedruckt. Bitte senden Sie diese zur Freischaltung unterschrieben an die Bank.

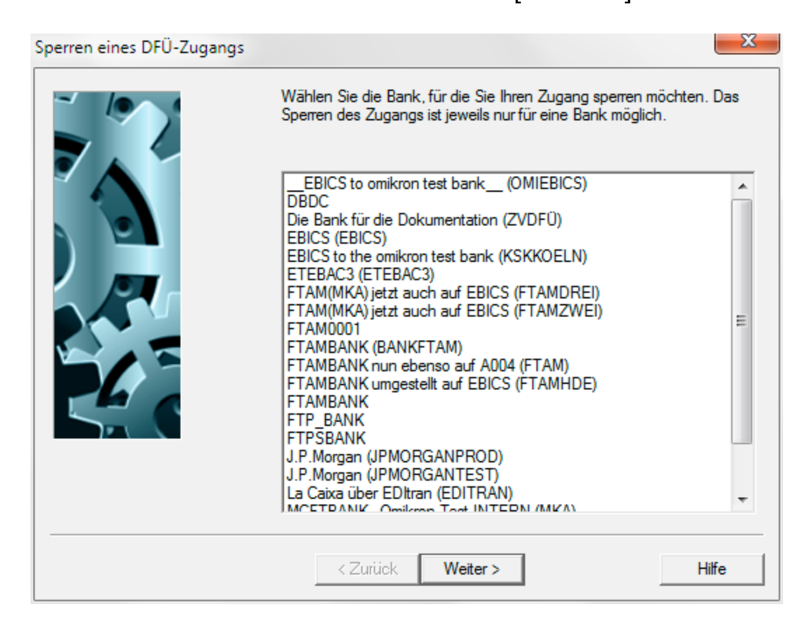


4.4 Sperren eines DFÜ-Zugangs (Sessiontyp SPR)

Um einen Bankzugang zu sperren, wählen Sie im Menü -Kommunikation- den Menüpunkt - Sperren eines DFÜ-Zugangs-.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um einen DFÜ-Zugang zur Bank zu sperren. Das Sperren ist jeweils nur für eine Bank möglich.

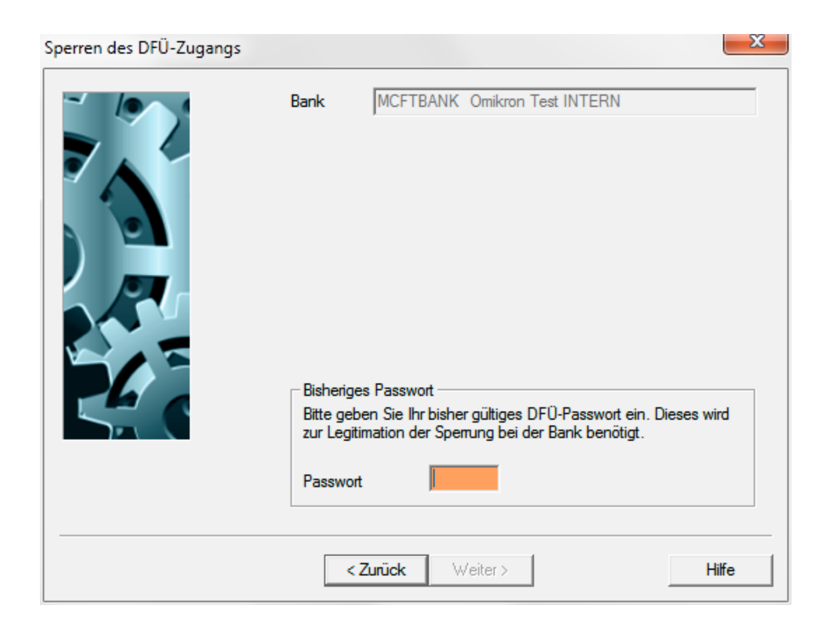
1 **Auswahl der Bank**
Wählen Sie die Bank aus der Liste mittels Mausklick aus, für die Sie den DFÜ-Zugang sperren möchten. Drücken Sie anschließend auf die Schaltfläche [***Weiter*** **>**].



nur bei EBICS:
Ist der Teilnehmerstatus abweichend von "Bereit", erscheint hier bei EBICS eine Warnmeldung. Ansonsten folgt direkt Punkt 2.

2 **Sperren des DFÜ-Zugangs**
Bei EBICS muss der Auftrag zur Sperrung vom zu sperrenden Teilnehmer signiert werden. Geben Sie daher im Bereich "Signieren der Teilnehmersperrung" Ihr aktuell gültiges "**EU-Passwort**" für die Elektronische Unterschrift in das entsprechende Feld ein. Die Abfrage des EU-Mediums erfolgt im letzten Schritt (-> **3**) des Assistenten.
Im unteren Bereich müssen Sie das gültige DFÜ-**Passwort** eingeben. Es wird zur Legitimation der Sperrung bei der Bank benötigt.

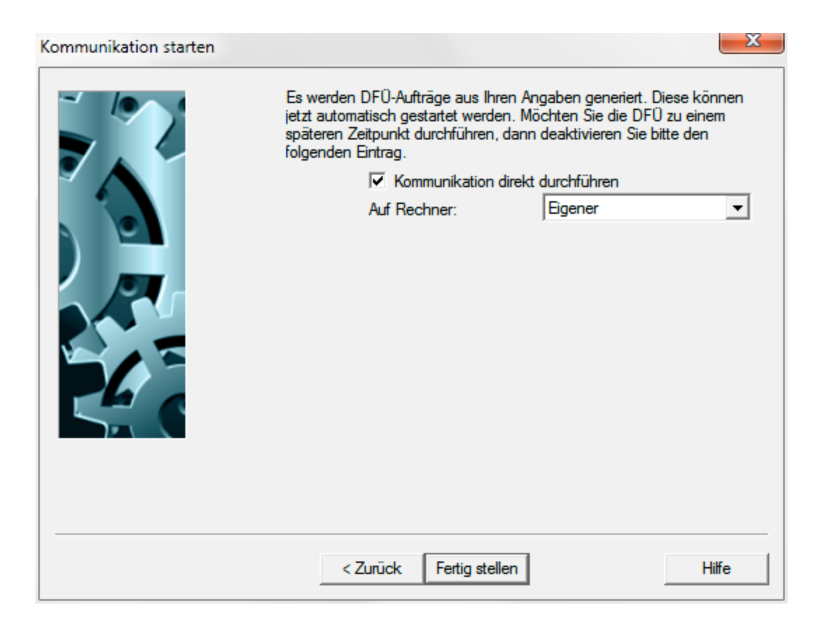




Sie tragen das DFÜ-Passwort in das entsprechende Feld. Die Passwortvergabe erfolgt verdeckt, d. h. jeder Tastendruck wird durch ein * (Sternchen) dargestellt. Sie schließen die Passworteingabe ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.

3 **Kommunikation starten**

Es werden DFÜ-Aufträge aus Ihren Angaben generiert. Diese können im letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen.
Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".
Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.



Über die Schaltfläche [**<** ***Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.



4.5 Verschlüsselung bei FTAM/FTP-Übertragungen

Das ZVDFÜ/MCFT-Verfahren beinhaltet automatisch eine Datenverschlüsselung. Bei Übertragung von Daten via FTAM haben Sie die Option, ihre Daten zu verschlüsseln, bei FTP werden die Daten generell verschlüsselt. Bei dem hierbei verwendeten Verschlüsselungsverfahren handelt es sich um ein sogenanntes Hybrid-Verfahren, das auf einer Kombination von DES- und RSA-Verschlüsselung basiert. Die zu übertragenden Nachrichten werden DES verschlüsselt und der verwendete DES-Schlüssel wird RSA-verschlüsselt in einem Vorsatz der Nachricht übertragen.

Weitere Informationen zum Thema der Verschlüsselung von per FTAM/FTP übertragenen Daten finden Sie im Kapitel 1.2.3: *FTAM*. Dort finden Sie auch eine schematische Darstellung der Vorgänge bei der Verschlüsselung.

Als Voraussetzung für die Datenverschlüsselung muss der jeweilige Empfänger der verschlüsselten Daten dem Sender dieser Daten den öffentlichen Schlüssel seines RSA-Verschlüsselungs-Key-Paares bekannt machen. Im Rahmen der Kunde-Bank-Beziehung übermitteln Sie Ihren Verschlüsselungs-Public Key der Bank unter Nutzung der Auftragsart **VPK** (Versand Public Key Kunde).
Der bankseitige Verschlüsselungs-Public-Key wird Ihnen unter Nutzung der Auftragsart **VPB** (Versand Public Key Bank) von der Bank zur Verfügung gestellt.

Die für die Verschlüsselung notwendigen Einstellungen, die Sie unter dem Menüpunkt -Kommunikation-, -Verschlüsselung- vornehmen, sind im folgenden Kapitel näher erläutert:

Kapitel 4.5.1: *Verschlüsselung mit Banken in Betrieb nehmen*

Spezielle, bei der Verschlüsselung gebräuchliche Returncodes finden Sie im

Kapitel 4.5.2: *DFÜ-Returncodes im Rahmen der Verschlüsselung*



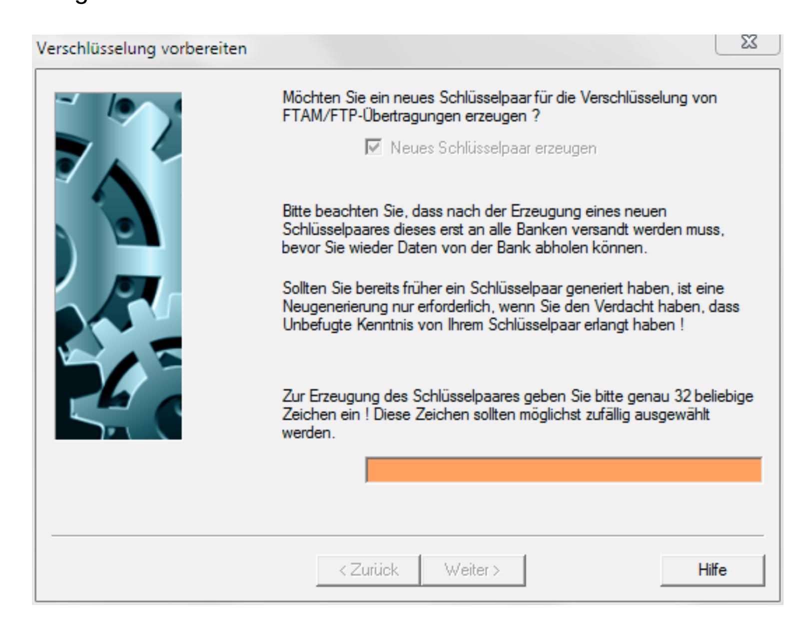
4.5.1 Verschlüsselung mit Banken in Betrieb nehmen

Bei Anwahl des Menüpunktes -Kommunikation / -Verschlüsselung- wird -analog zur Verfahrensweise bei der Elektronischen Unterschrift (vgl. Kapitel 6.1: *EU-Schlüsselpaar generieren / versenden*)- das für die (mittels RSA-verschlüsselte) Übertragung des Verschlüsselungs-DES-Keys notwendige Verschlüsselungs-Key-Paar erzeugt.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um die Verschlüsselung in Betrieb zu nehmen.

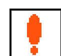
1 Erzeugen eines neuen Schlüsselpaares

Beachten Sie bitte:
Sollten Sie bereits früher ein Schlüsselpaar erzeugt haben, ist eine Neugenerierung nur erforderlich, wenn Sie den Verdacht haben, dass ein Unbekannter Kenntnis von Ihrem Schlüsselpaar erlangt haben könnte.



Zur Ermittlung des Schlüsselpaares geben Sie eine beliebige Zeichenkette bestehend aus exakt 32 Zeichen ein. Die **Zeichenkette** ist eine willkürliche Kombination aus Buchstaben, Zahlen und Sonderzeichen. Die Eingabe erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt. Diese frei wählbare Zeichenkette bildet die Basis zur Erstellung des Schlüsselpaares und die Zeichen sollten daher möglichst zufällig ausgewählt werden. Bei Eingabe von weniger als 32 Zeichen erhalten Sie eine entsprechende Fehlermeldung. Sie bestätigen Ihre Eingabe über die Schaltfläche [***Weiter*** **>**].

Beide Schlüsselteile (Secret und Public Key) werden verschlüsselt mit der internen User-ID und einem Zeitstempel auf Ihrer Festplatte im Verzeichnis ..\MCCWIN\DAT abgelegt.
Über einen Parametereintrag (V_KEY_DRIVE) in der Steuerdatei CSUB.PRO haben Sie die Möglichkeit, den Verschlüsselungs-Secret-Key auch auf einem anderen Laufwerk abzulegen.

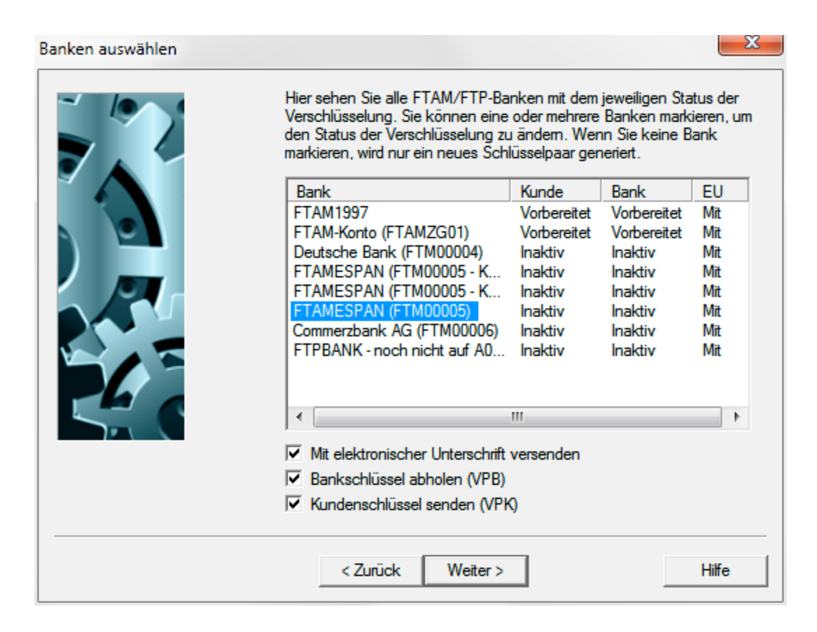


Normalerweise ist eine erneute Generierung eines Schlüsselpaares für die normale Nutzung des Programmes nicht erforderlich. Sollten Sie den Schlüssel ändern, müssen Sie diese Änderung durch einen Auftrag VPK allen Banken, mit denen Sie kommunizieren, mitteilen, d. h. nach der Erzeugung eines neuen Schlüsselpaares **muss dieses erst an alle Banken versandt werden, bevor Sie wieder Daten von Ihrer Bank abholen können**.



2 **Auswahl der Bank(en)**

Es wird Ihnen eine Liste der FTAM-(FTP-)Banken angeboten, zu denen automatisch ein "VPK"- oder ein "VPB"-DFÜ-Auftrag generiert werden soll. Der jeweilige Status der Verschlüsselung ist angegeben. Als Verschlüsselungsverfahren mit der Bank wird standardmäßig das Triple-DES-Verfahren verwendet.



Wählen Sie die Bank(en) aus der Liste mittels Mausklick aus, für die Sie ein Schlüsselpaar generieren möchten. Sie können eine oder mehrere Banken markieren, um den Status der Verschlüsselung zu ändern. Wenn Sie keine Bank markieren, wird nur ein neues Schlüsselpaar generiert.

Das Markieren des Feldes "**Mit elektronischer Unterschrift versenden**" kommt nur dann zum Tragen, wenn Sie zum Basismodul auch das Zusatzmodul **EU** (= Elektronische Unterschrift) installiert haben und die Daten mit dem FTAM-(FTP-)Verfahren zur Bank übertragen wollen. Informationen zur EU enthält die Dokumentation zum DFÜ-Modul (Kapitel 6: *Elektronische Unterschrift*).
Möchten Sie die Datei vor der Durchführung der Übertragung mit einer elektronischen Unterschrift versehen werden soll, markieren Sie das Kästchen vor dem Feld "Mit elektronischer Überschrift versenden" (Standardbelegung).

Die weiteren Kontrollkästchen "**Bankschlüssel abholen (VPB)**" und "**Kundenschlüssel senden (VPK)**" werden entsprechend den aktuellen Verschlüsselungs-Stati (kunden- / bankseitig) vorbelegt, können bei Bedarf jedoch angepasst werden.
Diese Auswahlmöglichkeit besteht nur dann, wenn genau eine Bank(parameterdatei) ausgewählt wurde. Sobald mehr als eine Bank markiert wird, werden die beiden Kontrollkästchen ausgeblendet, da dann die Kommunikationsaufträge automatisch dem Status der BPD entsprechend generiert werden.

Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].

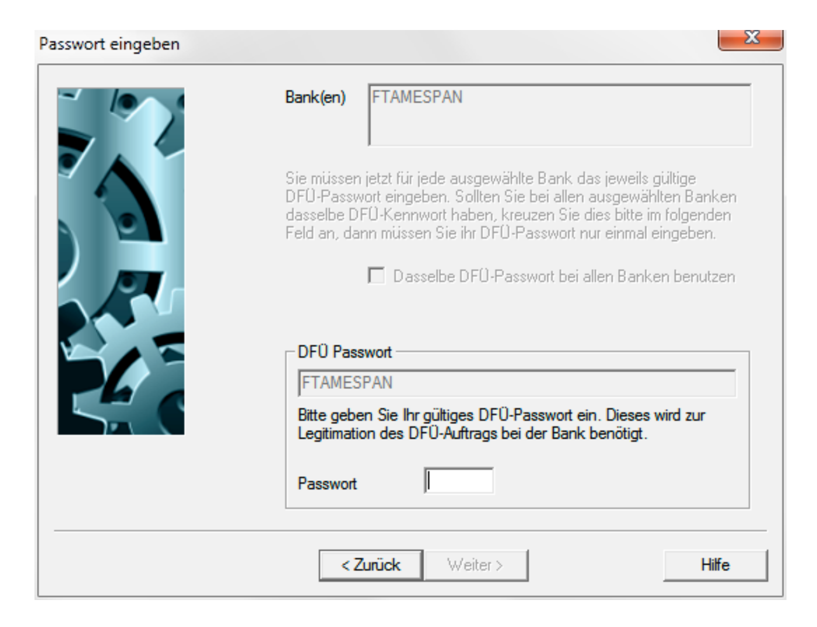
3 **DFÜ-Passwort eingeben**

Unterhalb der ausgewählten Bank(en) müssen Sie nun das gültige DFÜ-Passwort eingeben. Es wird zur Legitimation der Schlüsseländerung bei der Bank benötigt.

Damit die auf der Festplatte gespeicherte Datei per DFÜ an Ihr Kreditinstitut übertragen werden kann, muss die Datei zur Absicherung mit einem DFÜ-Passwort versehen sein.



Dieses DFÜ-Passwort ist nur Ihnen bekannt und wird von Ihnen bei der Installation des Verbindungsweges zwischen Ihrem Rechner und dem Kreditinstitut festgelegt. Falls erforderlich, kann dieses DFÜ-Passwort jederzeit geändert werden. Die Festlegung und Änderung des DFÜ-Passwortes ist nur über das DFÜ-Programm des Basismoduls möglich. Informationen dazu erhalten Sie in der Dokumentation zum DFÜ-Modul (s. Kapitel 5.1.1: Datenbankübersicht Datei-Manager*: Registerkarte "Passwort und Ausführungsdaten"*).



Haben Sie mehrere Banken ausgewählt, können Sie durch Markieren des Kontrollkästchens "**Dasselbe DFÜ-Passwort bei allen Banken benutzen**" bestimmen, dass bei allen Banken dasselbe DFÜ-Passwort verwendet wird. Andernfalls lassen Sie diese Option unmarkiert. Es wird dann anschließend für jede gewählte Bank das aktuell gültige DFÜ-Passwort abgefragt.

☞ **Beachten Sie bitte:**

Die Bank(parameterdatei) kann oberhalb des Passwort-Eingabefeldes nur angezeigt werden, wenn in der jeweiligen Bankparameterdatei das Feld "Bezeichnung der Bankparameterdatei" gefüllt wurde.

Sie tragen das DFÜ-Passwort in das entsprechende Feld. Die Passwortvergabe erfolgt verdeckt, d. h. jeder Tastendruck wird durch ein * (Sternchen) dargestellt. Sie schließen die Passworteingabe ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.

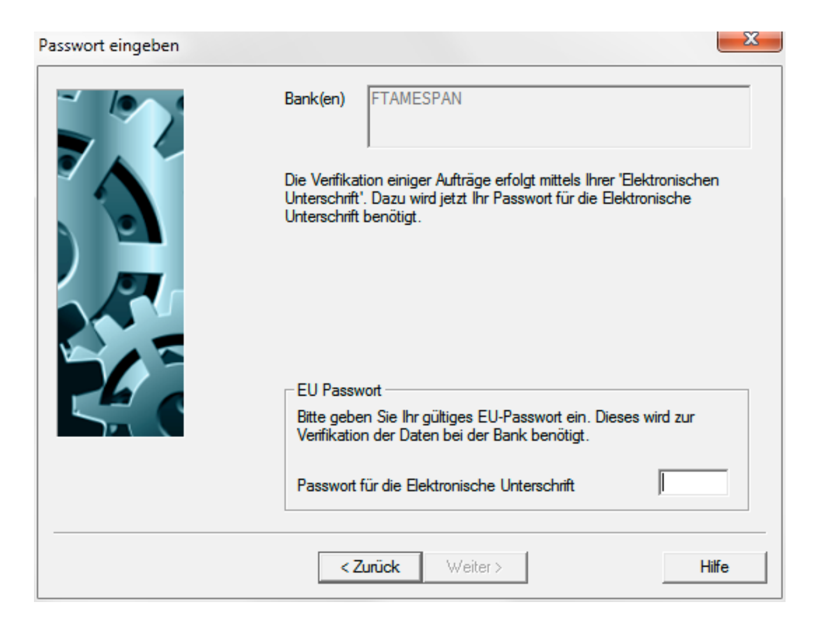
4 EU-Passwort eingeben

Auf die Eingabe des DFÜ-Passwortes folgt, sofern Sie den Parameter "Mit elektronischer Unterschrift" markiert haben (s. o.), die Eingabe des Passwortes für die Elektronische Unterschrift.

Um anschließend die Elektronische Unterschrift leisten zu können, werden Sie aufgefordert, das EU-Passwort einzugeben. Das **EU-Passwort** wurde von Ihnen bei der Generierung des Schlüsselpaares zur Verschlüsselung des Private Keys auf der Schlüsseldiskette gewählt (s. Kapitel 6.1: *EU-Schlüsselpaar generieren / versenden*).

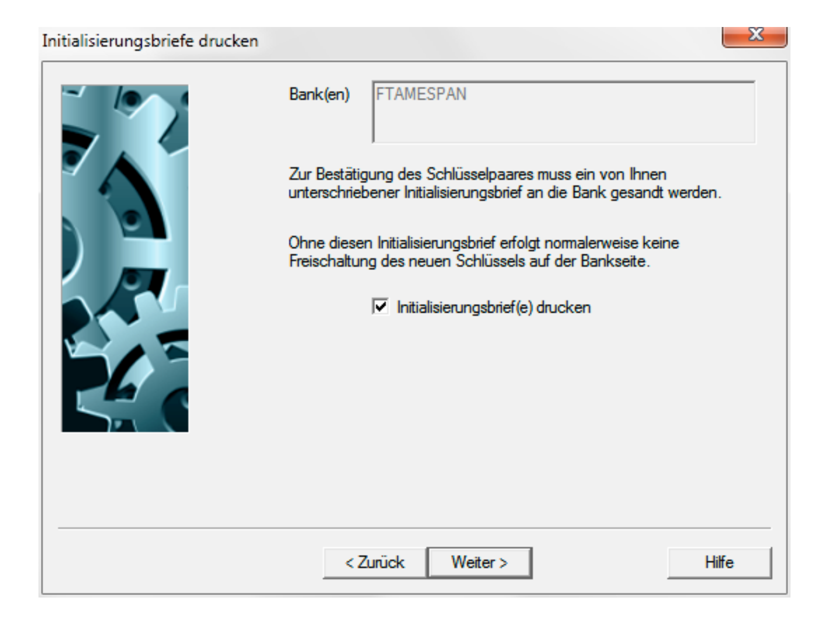
Sie bestätigen Ihre Eingaben durch Betätigen der Schaltfläche [***Weiter >***].





5 **Initialisierungsbrief(e) drucken**

Zur Bestätigung des (neuen) Schlüsselpaares muss ein von Ihnen unterschriebener Initialisierungsbrief an die Bank (oder an mehrere) gesandt werden, mit der (denen) Sie ohne **E**lektronische **U**nterschrift arbeiten. Ohne diesen Initialisierungsbrief erfolgt normalerweise keine Freischaltung des neuen Schlüssels auf der Bankseite. Die Option "**Initialisierungsbrief(e) drucken**" ist bereits markiert.

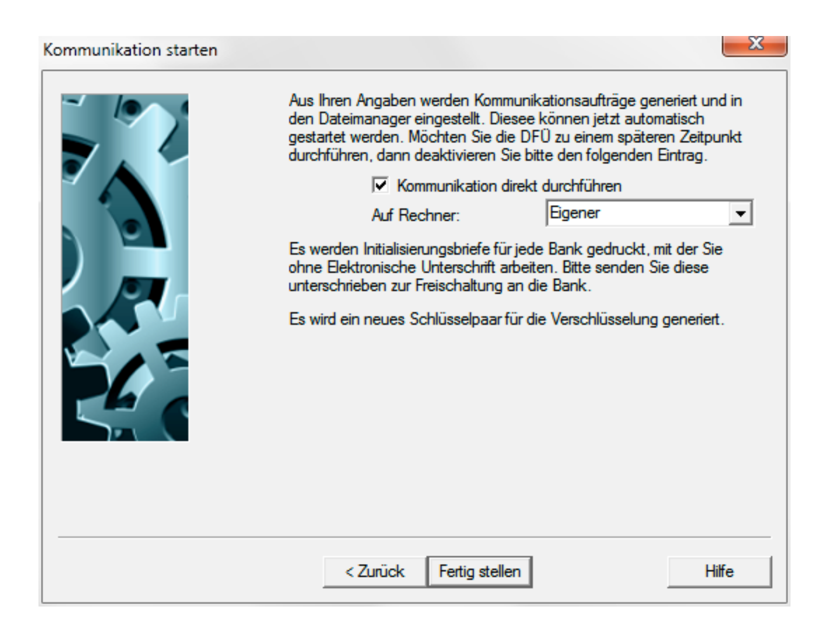


Möchten Sie keine(n) Initialisierungsbrief(e) drucken, entfernen Sie bitte die entsprechende Markierung.

6 **Kommunikation starten**

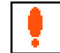
Es wird eine DFÜ-Auftragsdatei aus Ihren Angaben generiert. Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".
Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.





Über die Schaltfläche [***< Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.

Es wird zunächst das neue Schlüsselpaar für die Elektronische Unterschrift generiert. Legen Sie hierzu bitte ein Speichermedium ein und schließen Sie den Hinweis darauf mit [***OK***]. Befindet sich bereits ein Private Key auf dem Speichermedium, erfolgt eine Sicherheitsabfrage, ob dieser überschrieben werden soll. Wählen Sie [***Ja***], wird der bisherige Private Key überschrieben. Soll dies nicht geschehen, wählen Sie [***Nein***] und legen eine neue Diskette ein.



Bewahren Sie das Schlüsselmedium **immer** an einem sicheren Ort auf.

Das Programm fordert Sie anschließend auf, das Schlüsselmedium in das bei der Installation des EU-Moduls definierte Laufwerk einzulegen, so dass das Schlüsselmedium anhand des EU-Passwortes geprüft werden kann.

Nach Bestätigen mit [***OK***] und nach erfolgreicher Durchführung der Elektronischen Unterschrift startet die Kommunikation.

Die DFÜ-Aufträge zum Versenden der Public Keys werden temporär erzeugt und nach der Abarbeitung der DFÜ wieder gelöscht.

Sobald die Bank eine erfolgreiche Authentifizierung des (neuen) VPKs vornehmen konnte, werden die bankseitig bereitgestellten Daten mit Ihrem (neuen) VPK verschlüsselt und Sie werden für die mit Ihrer Bank vereinbarten Abholauftragsarten freigeschaltet. Der Public Key der Bank wird auf Ihrer Festplatte in der BPD-Datei abgelegt.

Bei einer nicht erfolgreichen Authentifizierung des VPK-Auftrages erhalten Sie beim Abholversuch einer verschlüsselt vereinbarten Auftragsart von Ihrer Bank den Antwortcode 54 zurück: "Verschlüsselungscode muss neu verschickt werden". Ausserdem wird sich Ihre Bank mit Ihnen zur Problembeseitigung gesondert in Verbindung setzen.

Sollten nicht alle Aufträge zur Aktivierung der Verschlüsselung erfolgreich durchgeführt worden sein (z. B. aufgrund eines wiederholten Besetztfalls), so werden Sie durch eine entsprechende Meldung darauf hingewiesen, dass der Menüpunkt -Verschlüsselung- erneut anzuwählen ist.

Abschließende Hinweise (wie z. B. auf die Erstellung eines DFÜ-Auftrags zum späteren Versenden des Schlüssels) quittieren Sie durch Drücken von [***OK***].



Anschließend werden Initialisierungsbriefe für jede ausgewählte Bank, mit der ohne EU gearbeitet werden soll, gedruckt. Bitte senden Sie diese unterschrieben zur Freischaltung des Schlüsselpaares an die Bank.

☞ **Beachten Sie bitte:**

Sobald die Verschlüsselung mit einer Bank aktiviert ist, können ausser den EU-Dateien und den im folgenden aufgelisteten Auftragsarten alle übrigen Auftragsarten verschlüsselt übermittelt werden. Welche Auftragsarten im Einzelfall verschlüsselt übermittelt werden, ist Vereinbarungssache zwischen Ihnen und Ihrer Bank. Dies ist letztlich nur für Abhol-Auftragsarten relevant, da Sie bei Sende-Aufträgen die Möglichkeit haben, die Daten entweder verschlüsselt oder unverschlüsselt zu übermitteln.

Folgende (Verwaltungs-)Auftragsarten werden unverschlüsselt übertragen:

Kennung	Text
INI	Passwort-Initialisierung
PUB	Senden Public Key zur Unterschriftsverifizierung
PWA	Passwortänderung
SPR	Sperrung der Zugangsberechtigung
VPB	Abholen Public Key des Kreditinstitutes zur Verschlüsselung
VPK	Senden Public Key des Kunden zur Verschlüsselung



4.5.2 DFÜ-Returncodes im Rahmen der Verschlüsselung

Im Rahmen der Verschlüsselung werden banksystemseitig die nachfolgend aufgeführten Antwortcodes ausgegeben, die kundenseitig die entsprechend beschriebenen Aktionen auslösen, sofern diese im FTAM-Remote-Dateinamen die Versionskennung des Anwendungsprotokolles "A3" verwendet. (Ältere Kundensysteme, die mit der Versionskennung "A2" arbeiten, erhalten diese Antwortcodes grundsätzlich nicht.)

50 Aktion erfolgreich - Neue Bankparameterdaten abholen
Das Banksystem hat neue Bankparameterdaten zur Verfügung gestellt. Ihr System generiert automatisch einen BPD-Abholauftrag und informiert Sie darüber, dass der Abholauftrag automatisch gestartet wird.

51 Verschlüsselungscode mit Bank muss aktualisiert werden (Auftragsart VPB)
Auf dem Banksystem wurde ein neuer Verschlüsselungs-Public Key generiert, der von Ihrem System abgeholt werden muss. Sie werden darüber durch die Meldung "Bitte Menüpunkt -Verschlüsselung mit Bank in Betrieb nehmen- ausführen" hingewiesen. Solange der neue Verschlüsselungs-Public Key bei der Bank noch nicht abgeholt wurde, können Sie keine (verschlüsselten) Daten an die Bank übermitteln.

Der Antwortcode 51 kann auch dann vom Banksystem zurückgeliefert werden, wenn der im FTAM-Remote-Dateinamen der verschlüsselten Datei eingestellte Hashwert des verwendeten Verschlüsselungs-Public Key der Bank (VPB) nicht mit dem bankseitig erwarteten Hashwert übereinstimmt. In diesem Fall müssen Sie ebenfalls einen neuen Verschlüsselungs-Public Key bei der Bank abholen.

52 Daten müssen verschlüsselt abgeholt werden
Diese Meldung kann nur auftreten, wenn Sie versuchen, trotz einer aktivierten bankseitigen Verschlüsselung Daten unverschlüsselt abzuholen.

53 Daten müssen unverschlüsselt abgeholt werden
Diese Meldung kann nur auftreten, wenn Sie versuchen, Daten verschlüsselt abzuholen, obwohl diese bankseitig unverschlüsselt bereitgestellt werden.

54 Verschlüsselungscode muss neu verschickt werden (VPK)
Kundenseitig wird nach erfolgreichem Versand des VPK-Auftrages und des dazugehörigen Legitimationsauftrages zunächst davon ausgegangen, dass die entsprechende Authentifizierung bei der Bank mit positivem Ergebnis durchgeführt wurde. Verläuft die bankseitige Unterschriftsprüfung der VPK-Datei jedoch negativ, so erhält Ihr System beim Abholversuch von verschlüsselt vereinbarten Auftragsarten den obigen Antwortcode 54.

55 User nicht EU-berechtigt
Diese Meldung wird vom Banksystem zurückgeliefert, wenn beim Versand einer VPK-Datei mit Elektronischer Unterschrift festgestellt wird, dass der Unterschriftsberechtigte bei der Bank keine Unterschriftsberechtigung besitzt. Dies kann bereits bei der Übertragung der Datei selbst ermittelt werden, da die User-ID des Unterzeichnenden im FTAM-Remote-Dateinamen übergeben wird.

56 Verschlüsselungscode noch nicht freigegeben
Solange der kundenseitige Verschlüsselungs-Public Key bankseitig noch nicht authentifiziert ist, erhalten Sie bei dem Versuch, Daten mit den Auftragsarten abzuholen, für die die Verschlüsselung vereinbart wurde, den obigen Returncode 56.

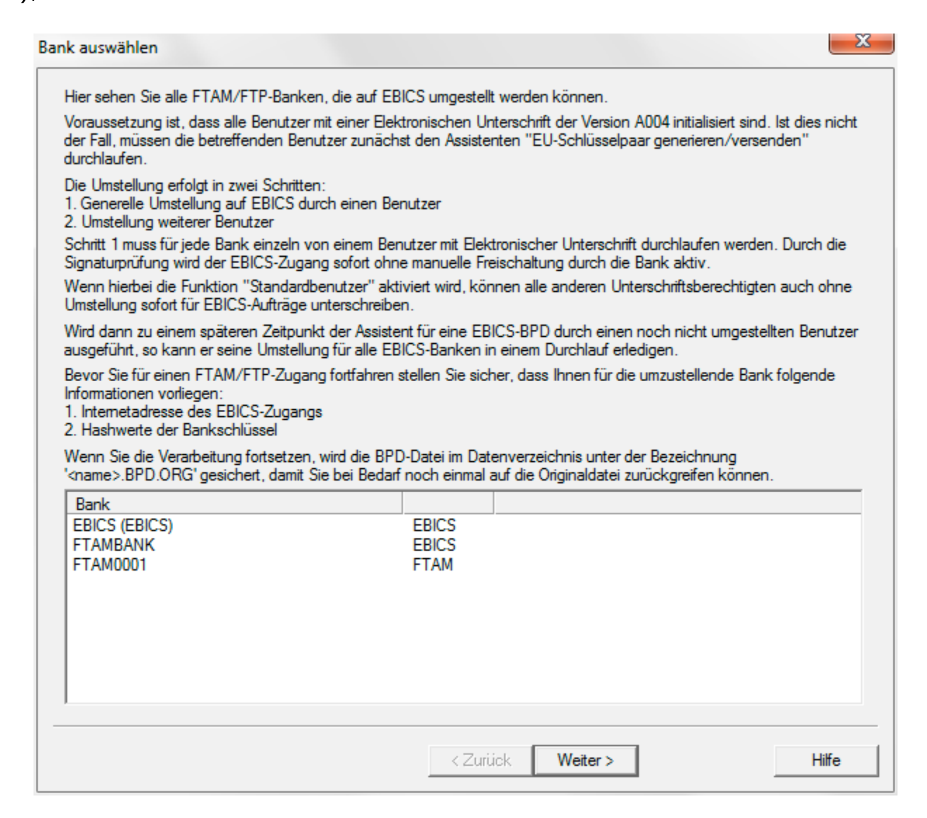


4.6 FTAM-/FTP-Bankzugang auf EBICS umstellen

Um einen bestehenden FTAM-/FTP-Bankzugang auf EBICS umzustellen, wählen Sie im Menü -Kommunikation- den Menüpunkt - FTAM-/FTP-Bankzugang auf EBICS umstellen-.

Ein Assistent geleitet Sie durch die notwendigen Schritte, um die Umstellung durchzuführen. Zunächst werden Sie aufgefordert, die umzustellende Bank auszuwählen.

1 **Bank auswählen**
Wählen Sie aus der Liste der Banken, die auf EBICS umgestellt werden können (FTAM-/FTP-BPDs mit EU-Version A004 sowie EBICS-BPDs mit Teilnehmerstatus ungleich "Bereit" oder "Gesperrt"), eine Bank mittels Mausklick aus.



Der Umstellungsassistent muss für jede FTAM- bzw. FTP-Bank **einzeln** durchlaufen werden. Wählen Sie mehr als eine Bank aus, erscheint eine Fehlermeldung:



☞ **Beachten Sie bitte:**
Voraussetzung für eine Umstellung ist, dass der betreffende Benutzer bei der umzustellenden Bank mit **einer Elektronischen Unterschrift der Version A004** initialisiert ist. Hat vorher keine Umstellung auf A004 stattgefunden, so kann später ein vollwertiger EBICS-Status nur durch Sperren des alten Zugangs und Erst-Initialisierung des neuen Zugangs erreicht werden.



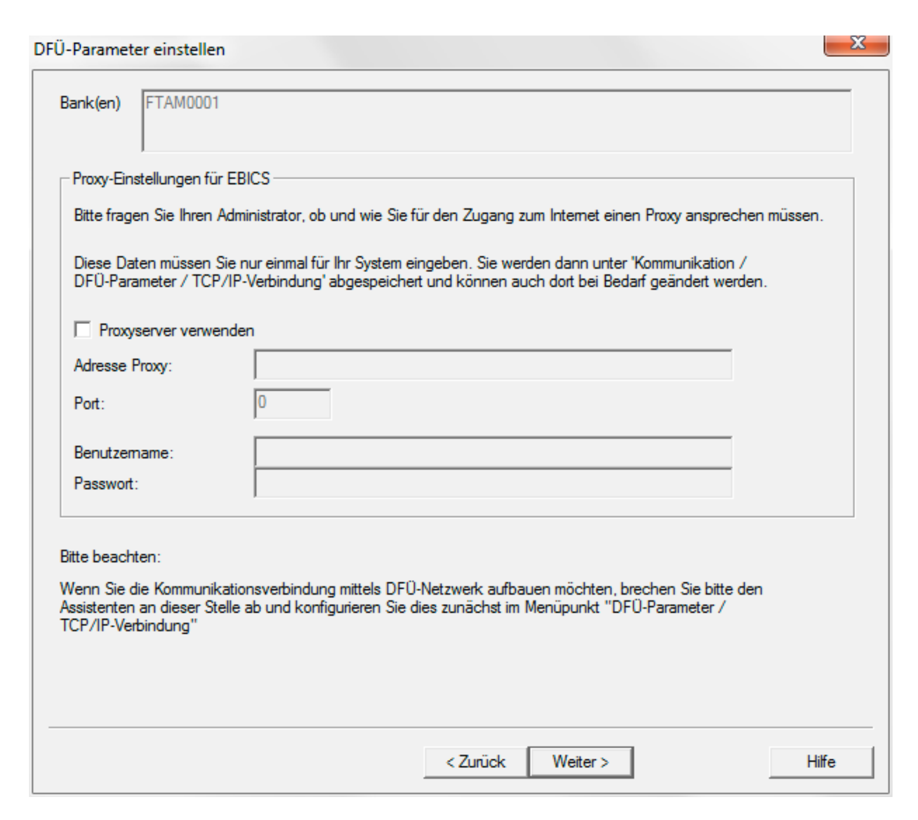
Die Umstellungsprozedur muss von nur einem Benutzer durchgeführt werden, sofern die übrigen Benutzer nur unterschreiben. Nach der Umstellung können diese Benutzer sofort weiterarbeiten. Sollen aus ihnen vollwertige EBICS-Teilnehmer werden, d. h. die auch selber Kommunikationsaufträge erstellen, so muss jeder von ihnen diesen Assistenten durchlaufen. In diesem Fall können mehrere (z. B. durch einen ersten Benutzer) bereits umgestellte EBICS-Bankparameterdateien markiert werden.

Im Anschluss werden die neuen Authentifikationsschlüssel mit Elektronischer Unterschrift übertragen, so dass der Zugang sofort ohne Freischaltung durch die Bank aktiv wird.

Drücken Sie anschließend auf die Schaltfläche [***Weiter >***]. Die umgestellte Bankparameterdatei wird im Verzeichnis ..\DAT unter der Bezeichnung <BPDNAME>.BPD.ORG gespeichert, damit Sie bei Bedarf noch einmal auf diese Originaldatei zurückgreifen können.

2 DFÜ-Parameter einstellen (Proxy-Einstellungen für EBICS)

Wenn Sie für den Zugang zum Internet einen Proxy verwenden müssen, markieren Sie das entsprechende Kontrollkästchen. Die notwendigen Angaben zur **Adresse** und zum **Port** des Proxy stellt Ihnen Ihr Administrator zur Verfügung. Weiterhin kann für den Zugang zum Proxy ein **Benutzername** und ein **Passwort** erfasst werden.



Die Proxy-Einstellungen werden nur dann zur Eingabe angeboten, wenn diese in den DFÜ-Parametern noch nicht festgelegt wurden (s. Kapitel 2.6: *Registerkarte TCP/IP-Verbindung*). Die im Assistenten erfassten Angaben werden in den DFÜ-Parametern gespeichert und beim nächsten Durchlauf des Assistenten nicht mehr abgefragt.

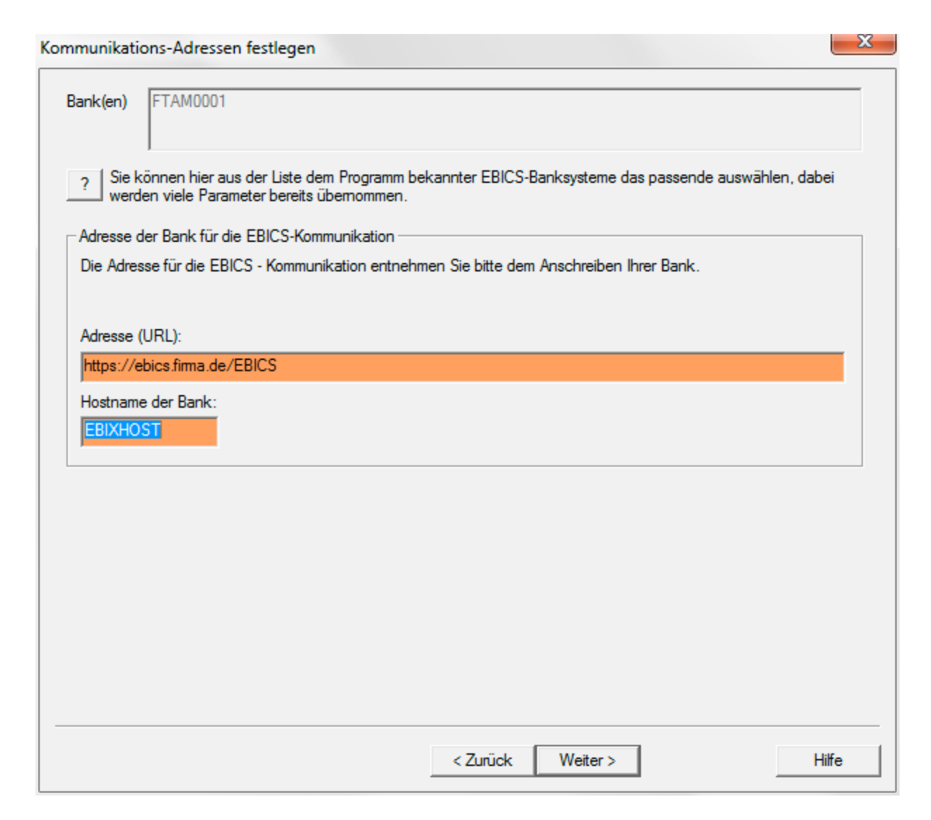
Beachten Sie bitte:
Wenn Sie die Kommunikationsverbindung mittels DFÜ-Netzwerk aufbauen möchten, brechen Sie bitte den Assistenten an dieser Stelle ab und konfigurieren Sie dies zunächst auf der oben genannten Registerkarte.

Sie schließen die Eingaben durch Drücken der Schaltfläche [***Weiter >***] ab.



3 **EBICS-Kommunikationsadresse festlegen**

Über die [**?**]-Schaltfläche können Sie eine Liste bekannter EBICS-Bankzugangsdaten aufrufen. Sofern ein passender Zugang in der alphabetischen Liste enthalten ist, können Sie diesen auswählen und die Zugangsdaten durch Betätigen der Schaltfläche [***Speichern***] in die Bankparameterdatei übernehmen.



Sofern der Bankzugang nicht in der Liste enthalten ist, geben Sie im Feld "**Adresse (URL)**" die für die EBICS-Kommunikation vorgesehene Internet-Adresse der betreffenden Bank ein. Diese entnehmen Sie den von der Bank zur Verfügung gestellten Unterlagen.

Weiterhin ist der **Hostname der Bank** (für den EBICS-Prozess) anzugeben. Bei älteren Releases (vor Version 3.21.005) ist der Hostname für EBICS vor der Umstellung direkt in die Bankparameterdatei einzugeben, sofern der EBICS-Hostname von dem für FTAM/FTP abweicht.

Sie schließen die Eingaben ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.

4 **Standardbenutzer (=Technischen Benutzer) definieren**

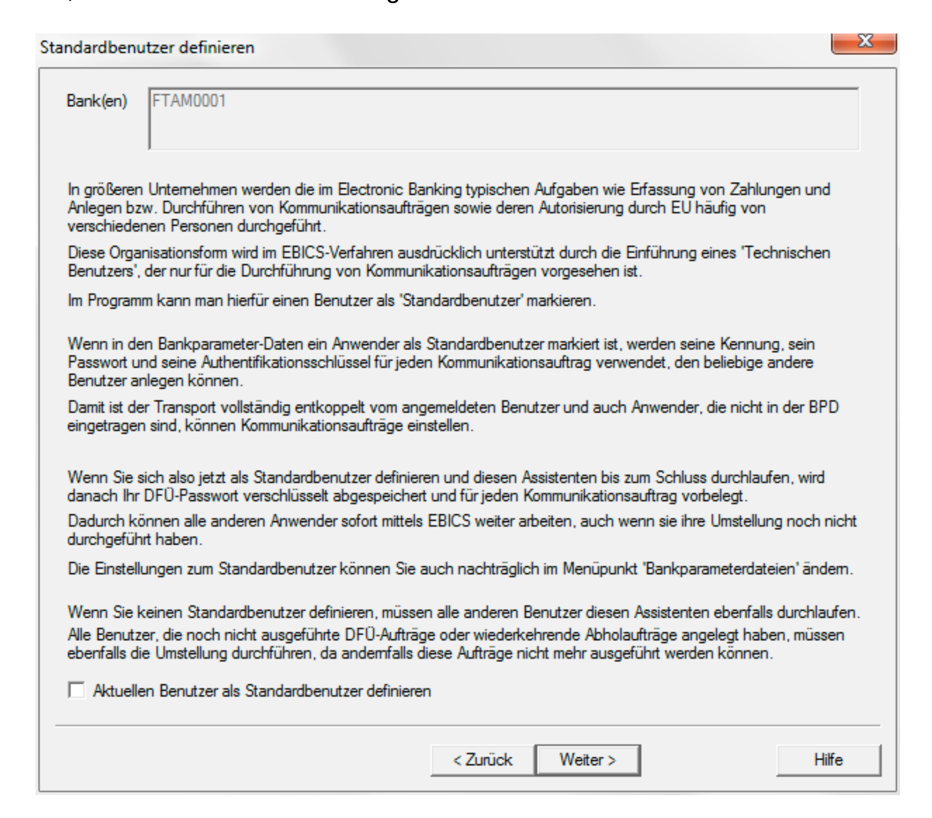
In größeren Unternehmen werden die im Electronic Banking typischen Aufgaben wie Erfassung von Zahlungen und Anlegen bzw. Ausführen von Kommunikationsaufträgen sowie deren Autorisierung durch EU häufig von verschiedenen Personen durchgeführt. Diese Organisationsform wird im EBICS-Verfahren ausdrücklich unterstützt durch die Einführung eines "Technischen Benutzers", der nur für die Ausführung von Kommunikationsaufträgen vorgesehen ist.

Im Programm kann man hierfür einen Benutzer als "Standardbenutzer" kennzeichnen. Ist in den Bankparameterdaten ein Anwender als Standardbenutzer gekennzeichnet, werden seine Kennung, sein Passwort und seine Authentifizierungsschlüssel für jeden Kommunikationsauftrag verwendet, den beliebige andere Benutzer anlegen können. Damit ist der Transport vollständig



entkoppelt vom angemeldeten Benutzer und auch Anwender, die nicht in der BPD eingetragen sind, können Kommunikationsaufträge einstellen.

Markieren Sie das Kontrollkästchen "**Aktuellen Benutzer als Standardbenutzer definieren**" ganz unten auf der Seite, definieren Sie sich als Standardbenutzer. Nach Durchlaufen des Assistenten wird Ihr DFÜ-Passwort verschlüsselt abgespeichert und für jeden Kommunikationsauftrag vorbelegt. Dadurch können alle anderen Anwender sofort weiterarbeiten, ohne selbst die Umstellung auf EBICS durchführen zu müssen.


Standardbenutzer definieren

Bank(en) FTAM0001

In größeren Unternehmen werden die im Electronic Banking typischen Aufgaben wie Erfassung von Zahlungen und Anlegen bzw. Durchführen von Kommunikationsaufträgen sowie deren Autorisierung durch EU häufig von verschiedenen Personen durchgeführt.

Diese Organisationsform wird im EBICS-Verfahren ausdrücklich unterstützt durch die Einführung eines 'Technischen Benutzers', der nur für die Durchführung von Kommunikationsaufträgen vorgesehen ist.

Im Programm kann man hierfür einen Benutzer als 'Standardbenutzer' markieren.

Wenn in den Bankparameter-Daten ein Anwender als Standardbenutzer markiert ist, werden seine Kennung, sein Passwort und seine Authentifikationsschlüssel für jeden Kommunikationsauftrag verwendet, den beliebige andere Benutzer anlegen können.

Damit ist der Transport vollständig entkoppelt vom angemeldeten Benutzer und auch Anwender, die nicht in der BPD eingetragen sind, können Kommunikationsaufträge einstellen.

Wenn Sie sich also jetzt als Standardbenutzer definieren und diesen Assistenten bis zum Schluss durchlaufen, wird danach Ihr DFÜ-Passwort verschlüsselt abgespeichert und für jeden Kommunikationsauftrag vorbelegt.

Dadurch können alle anderen Anwender sofort mittels EBICS weiter arbeiten, auch wenn sie ihre Umstellung noch nicht durchgeführt haben.

Die Einstellungen zum Standardbenutzer können Sie auch nachträglich im Menüpunkt 'Bankparameterdateien' ändern.

Wenn Sie keinen Standardbenutzer definieren, müssen alle anderen Benutzer diesen Assistenten ebenfalls durchlaufen. Alle Benutzer, die noch nicht ausgeführte DFÜ-Aufträge oder wiederkehrende Abholaufträge angelegt haben, müssen ebenfalls die Umstellung durchführen, da andernfalls diese Aufträge nicht mehr ausgeführt werden können.

☐ Aktuellen Benutzer als Standardbenutzer definieren

< Zurück | Weiter > | Hilfe

Wenn Sie keinen Standardbenutzer definieren, müssen alle anderen Benutzer diesen Assistenten ebenfalls durchlaufen. Die Einstellungen zum Standarbenutzer können Sie auch nachträglich im Menüpunkt -Kommunikation- / -Bankparameterdateien- in der Bankparameterdatei umstellen (s. Kapitel 3.5: *EBICS*).

Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].

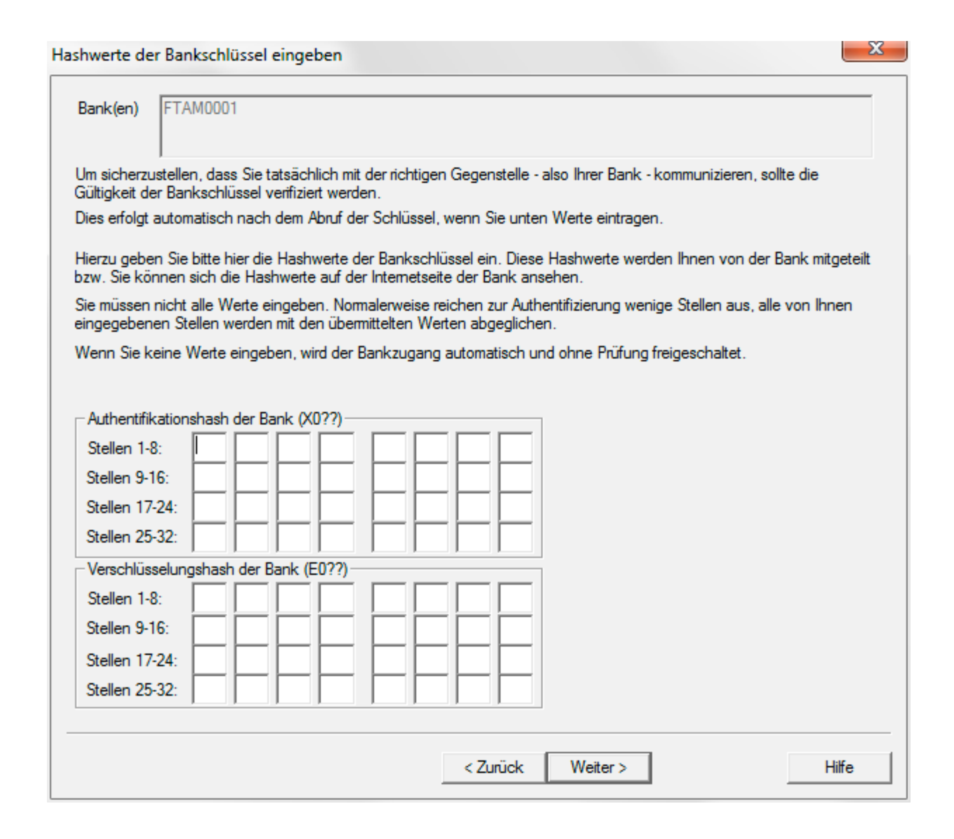
5 **Hashwerte der Bankschlüssel eingeben**

Um sicherzustellen, dass Sie tatsächlich mit der richtigen Gegenstelle -also Ihrer Bank- kommunizieren, sollte die Gültigkeit der Bankschlüssel, die am Ende dieses Assistenten abgeholt werden, verifiziert werden. Dies erfolgt automatisch nach Abruf der Schlüssel.

Geben Sie bitte dafür die Hashwerte der Bankschlüssel in die vorgesehenen Felder ein (**Authentifikationshash der Bank (X0??)** / **Verschlüsselungshash der Bank (E0??)**). Diese Hashwerte werden Ihnen von der Bank mitgeteilt bzw. Sie können sich die Hashwerte auf der Internetseite der Bank ansehen.

Sie müssen nicht alle Werte eingeben. Normalerweise reichen zur Authentifizierung wenige Stellen aus. Alle von Ihnen eingegebenen Werte werden mit den übermittelten Werten abgeglichen.
Die Werte im jeweils ersten Feld sind Pflicht, wenn sie von "00" abweichend sind.





Sie können den Status der Bankschlüssel im Menüpunkt -Kommunikation- / -Bankparameterdateien- in der Bankparameterdatei überprüfen und die Verifikation nachträglich durch Eingabe und Abspeichern der Hashwerte über die Schaltfläche [***Hashwerte der Bank***] wiederholen (s. Kapitel 3.5: *EBICS*).

Drücken Sie dann die Schaltfläche [***Weiter >***].

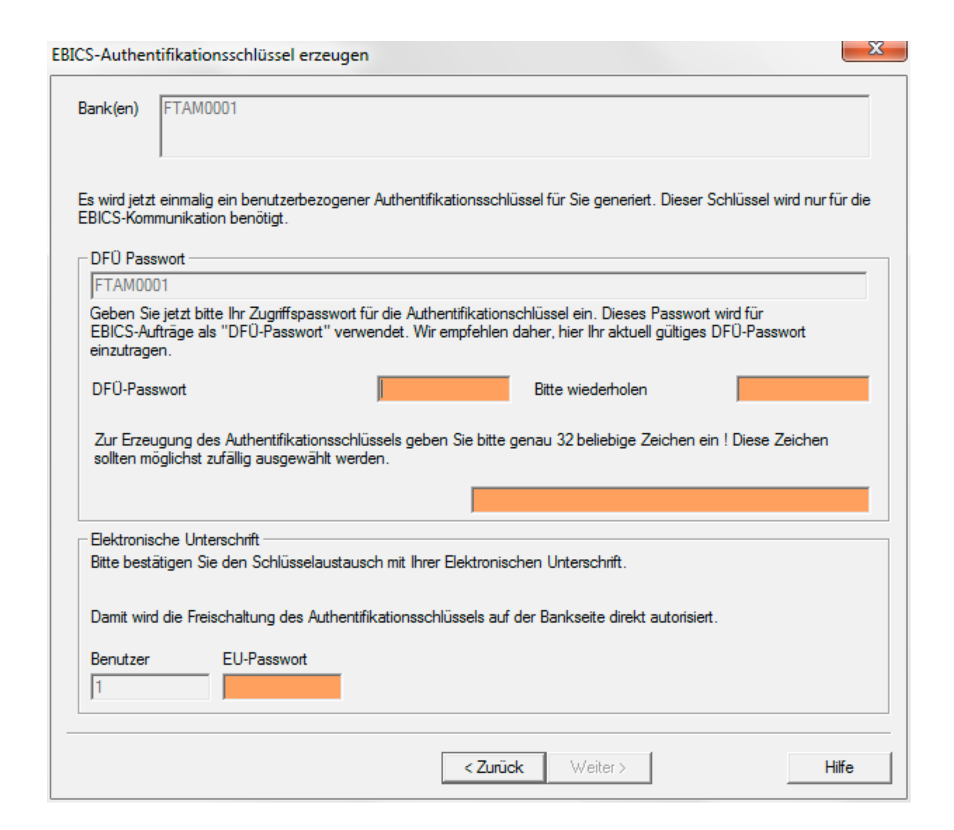
6a **EBICS-Authentifikationsschlüssel erzeugen** (beim erstmaligen Durchlaufen des Assistenten)
Durchlaufen Sie den Assistenten zum ersten Mal, wird **einmalig** ein benutzerbezogener Authentifizierungsschlüssel für Sie generiert. Dieser Schlüssel wird nur für die EBICS-Kommunikation benötigt.

Geben Sie bitte im Feld "**DFÜ-Passwort**" Ihr aktuell gültiges DFÜ-Passwort auch als neues Passwort für den Authentifizierungsschlüssel ein. Da die Passworteingabe verdeckt erfolgt, d. h. jeder Tastendruck durch ein * (Sternchen) dargestellt wird, müssen Sie die Passworteingabe zur Sicherheit im dafür vorgesehenen Feld **bitte wiederholen**.

Zur Erzeugung des Schlüsselpaares geben Sie bitte genau **32 beliebige Zeichen** ein. Diese Zeichenkette ist eine willkürliche Kombination aus Buchstaben, Zahlen und Sonderzeichen. Die Eingabe erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt.

Im Bereich "**Elektronische Unterschrift**" müssen Sie das neue Schlüsselpaar mit Ihrer Elektronischen Unterschrift bestätigen. Damit wird die Freischaltung des Schlüssels auf der Bankseite direkt autorisiert.





Geben Sie dazu Ihr "**EU-Passwort**" in das entsprechende Feld ein. Die Abfrage des EU-Mediums erfolgt im letzten Schritt (-> **7**) des Assistenten.

Drücken Sie abschließend die Schaltfläche [***Weiter >***].

6b **Passwort eingeben** (beim wiederholten Durchlaufen des Assistenten)
Beim erneuten Durchlaufen wird zunächst das "**Passwort**" für Ihren Authentifizierungsschlüssel abgefragt. Dieses wird zur Legitimation des Kommunikationsauftrages bei der Bank benötigt.

Anschließend müssen Sie im Bereich "Elektronische Unterschrift" das Schlüsselpaar mit Ihrer Elektronischen Unterschrift bestätigen. Damit wird die Freischaltung des Schlüssels auf der Bankseite direkt autorisiert.

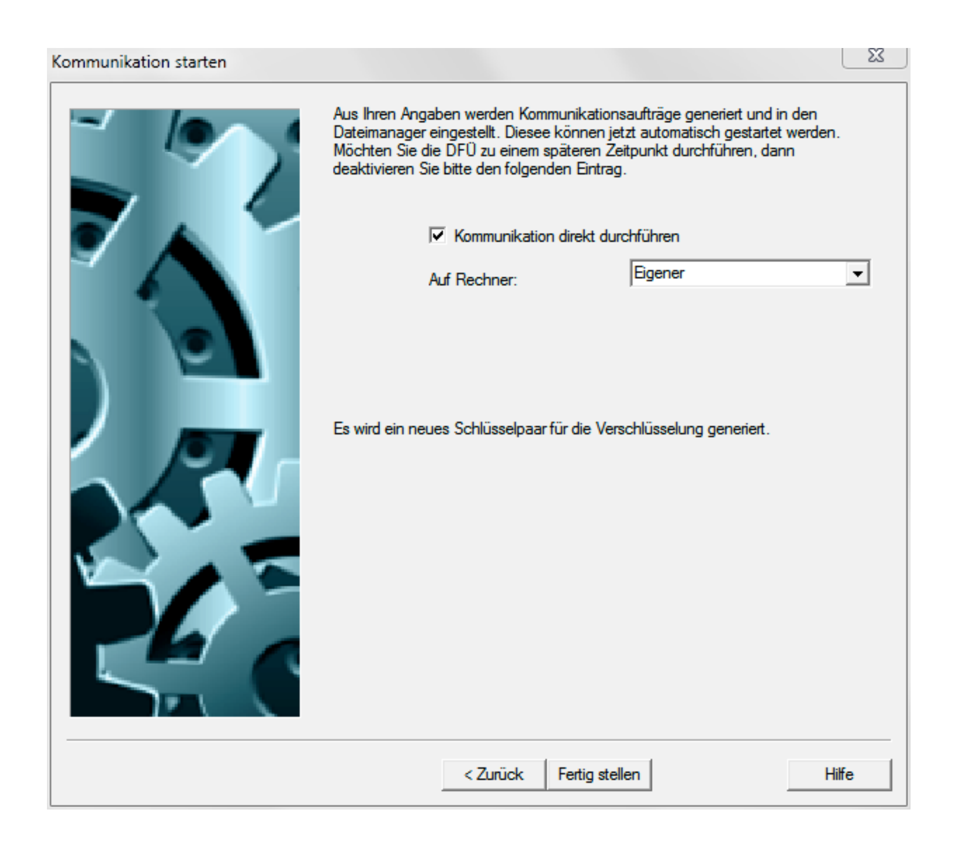
Geben Sie dazu Ihr "**EU-Passwort**" in das entsprechende Feld ein. Die Abfrage des EU-Mediums erfolgt im letzten Schritt (-> **7**) des Assistenten.

Drücken Sie dann die Schaltfläche [***Weiter >***].

7 **Kommunikation starten**
Es wird ein Kommunikationsauftrag/werden Kommunikationsaufträge aus Ihren Angaben generiert. Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".
Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.

Über die Schaltfläche [***< Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.





Zum Schluss werden die Kommunikationsaufträge HSA und HPB generiert und ggf. sofort ausgeführt.

Mit der Auftragsart HSA werden die Public Keys für die Authentifikation und Verschlüsselung signiert mit dem aktuellen bankfachlichen Schlüssel an die Bank übertragen. Der Public Key für die Elektronische Unterschrift (EU-Version A004) muss nicht mehr an die Bank geschickt werden, da dieser bereits im Rahmen des BCS-FTAM- bzw. BCS-FTP-Verfahrens genutzt wurde und bankseitig bereits vorliegt. Die Auftragsart HSA erfordert nicht den zusätzlichen Versand eines Initialisierungsbriefes, da die Authentizität der übermittelten Schlüssel durch die EU des betroffenen Teilnehmers gesichert wird.

Im Anschluss daran erfolgt die Abholung der Bankschlüssel mittels HPB mit automatischer Freischaltung.

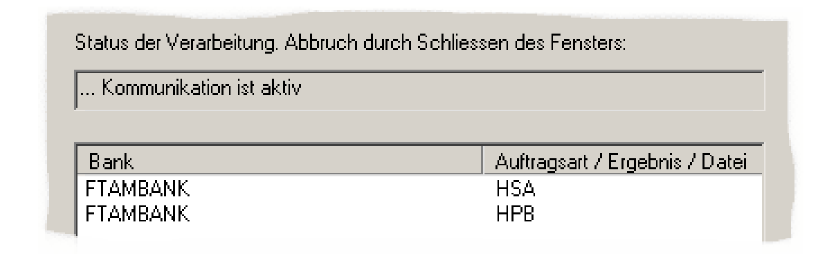
Da jeder EBICS-Kommunikationsauftrag mit einer Unterschrift versehen werden muss, erfolgt im Anschluss an das Drücken der Schaltfläche [***Fertig stellen***] die Aufforderung zur Eingabe des EU-Mediums. (Das EU-Passwort wurde ja bereits eingegeben.)

Nach Einlegen des EU-Mediums und Bestätigen mit [***OK***] wird in Abhängigkeit von dem oben erwähnten Kontrollkästchen die Kommunikation sofort oder später (d. h. aus dem Datei-Manager heraus) gestartet.

Im unterem Teil des Fensters erscheint dann eine Anzeige zum Status der Verarbeitung.



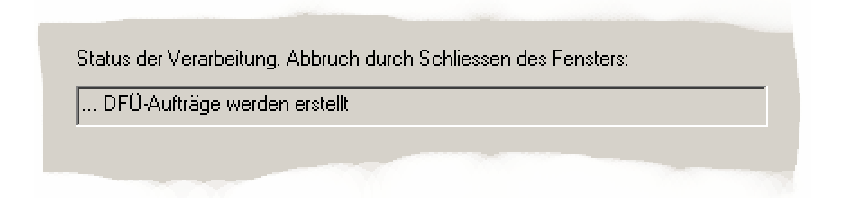
Kommunikation sofort:



Nach dem erfolgreichen Übertragen schließen Sie das erscheinende Hinweisfenster mit [***OK***].

Den Assistenten beenden Sie über ein abschließendes Drücken der Schaltfläche [***Fertig stellen***].

Kommunikation später:



Das erscheinende Hinweisfenster bestätigen Sie mit [***OK***]. Bearbeiten Sie die Kommunikationsaufträge mit dem entsprechenden Ordnungsbegriff anschließend im Datei-Manager weiter.



4.7 EBICS-Authentifikationsschlüssel austauschen

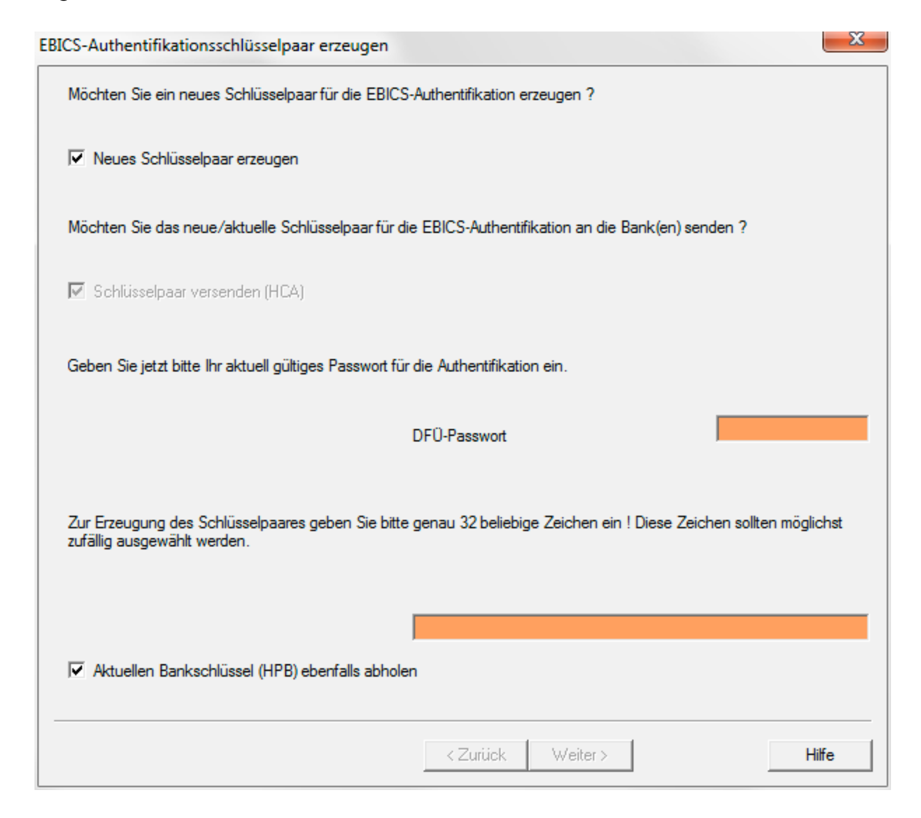
Um die EBICS-Authentifikationsschlüssel (A- und V-Key) zu ändern (zu erzeugen bzw. zu versenden) und/oder die entsprechenden Schlüssel der Bank erneut abzurufen, wählen Sie im Menü -Kommunikation- den Menüpunkt -EBICS-Authentifikationsschlüssel austauschen-.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um die EBICS-Authentifikationsschlüssel auszutauschen.

1 **EBICS-Authentifikationsschlüssel erzeugen/versenden**
Nach Aufruf des Menüpunktes ist das Kontrollkästchen "**Neues Schlüsselpaar erzeugen**" im Dialogfenster bereits markiert. Möchten Sie ein neues Schlüsselpaar für die EBICS-Authentifikation generieren, belassen Sie diese Voreinstellung.
Sollen dagegen bereits vorhandene (z. B. früher erzeugte) Schlüssel an die Bank(en) versandt werden, demarkieren Sie das oben genannte Kontrollkästchen.

Möchten Sie das neu erzeugte bzw. das aktuelle Schlüsselpaar an die Bank(en) senden, so belassen Sie auch hier die Markierung des Kontrollkästchens "**Schlüsselpaar versenden (HCA)**".
Über die Auftragsart HCA wird eine Anfrage zur Änderung der Teilnehmerschlüssel für Authentifikation und Verschlüsselung versandt. Demarkieren sie auch dieses Kontrollkästchen, können Sie den Assistenten nach Markieren der dritten Option zur Generierung eines HPB-Kommunikationsauftrages (s. unten) nutzen.

Zur Authentifizierung Ihres Auftrages/Ihrer Aufträge müssen Sie Ihr aktuell gültiges **DFÜ-Passwort** eingeben.



Sofern Sie das Kontrollkästchen zur Schlüsselpaarerzeugung (erste Option) markiert haben, müssen Sie daruter zur Erzeugung eines neuen Schlüsselpaares eine beliebige Zeichenkette bestehend aus exakt **32 Zeichen** eingeben. Diese Zeichen sollten möglichst zufällig ausgewählt werden. Die Eingabe erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein *



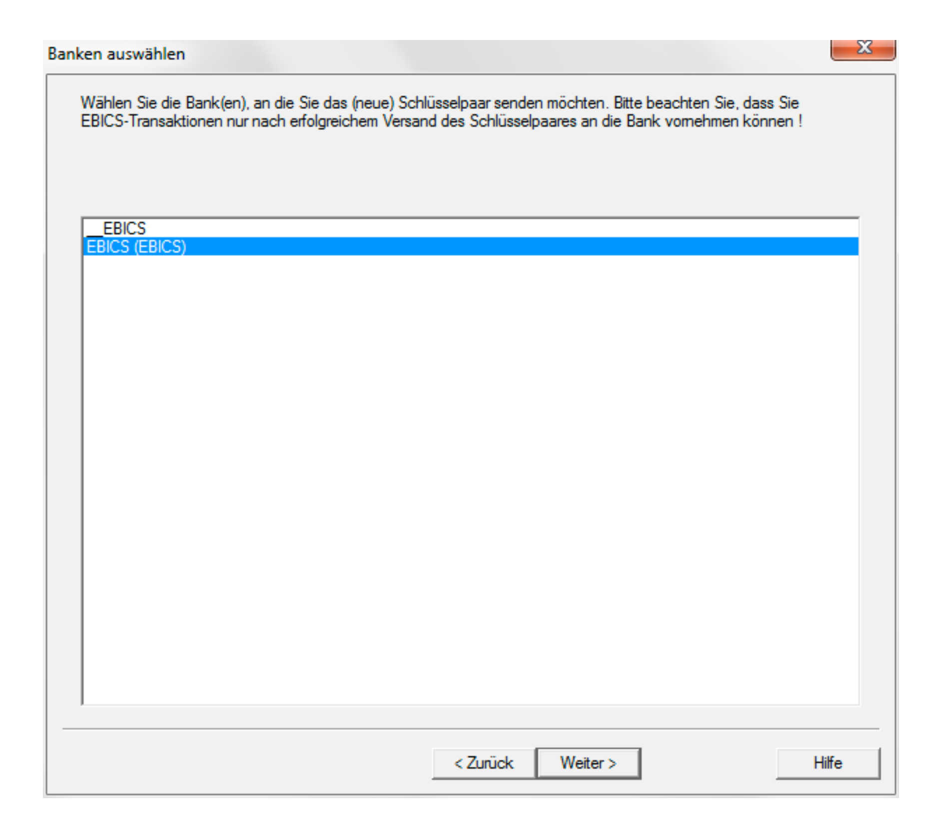
(Sternchen) dargestellt. Diese frei wählbare Zeichenkette bildet die Basis zur Erstellung des Schlüsselpaares.

Möchten Sie zusätzlich (oder ggf. ausschließlich) einen Kommunikationsauftrag mit dem Sessiontyp HPB anlegen, so ist das Kontrollkästchen "**Aktuellen Bankschlüssel (HPB) ebenfalls abholen**" zu markieren.
Über die Auftragsart HPB erfolgt der Transfer der öffentlichen Bankschlüssel.

Drücken Sie abschließend auf die Schaltfläche [***Weiter >***].

2 **Banken auswählen**

Es wird Ihnen eine Liste der EBICS-Banken angeboten. Wählen Sie die Bank(en) aus, an die Sie das (neue) Schlüsselpaar senden möchten. Biite beachten Sie, dass Sie EBICS-Transaktionen nur nach erfolgreichem Versand des Schlüsselpaares an die Bank vornehmen können!

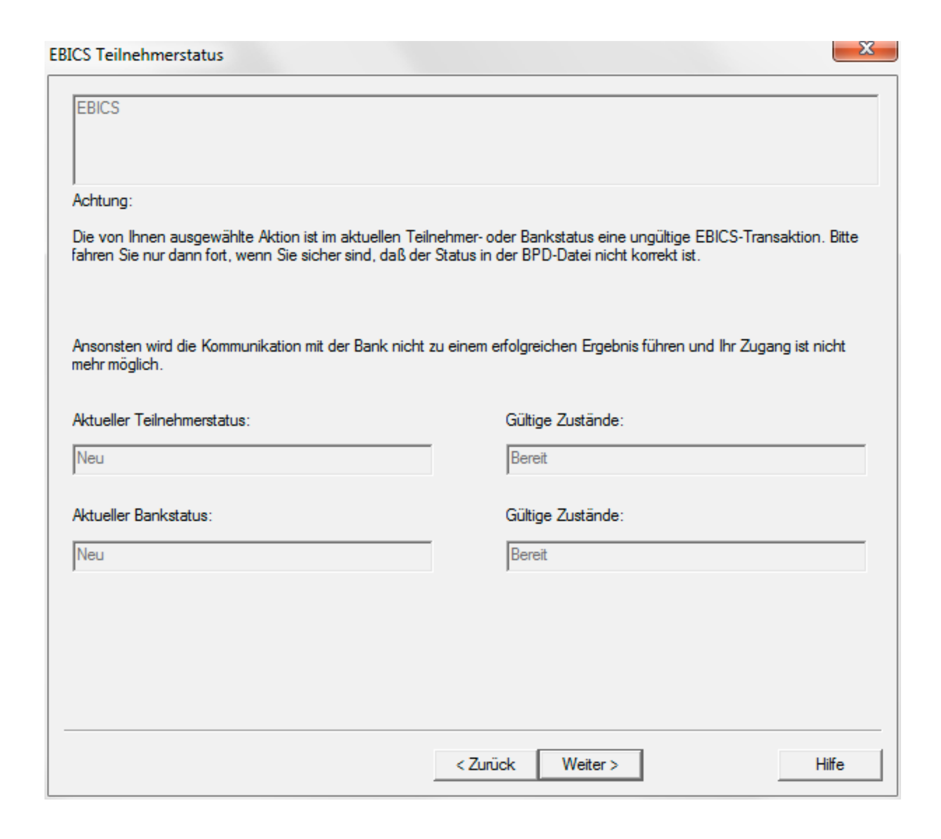


Anschließend klicken Sie auf die Schaltfläche [***Weiter >***].

3 **EBICS Teilnehmerstatus**

Handelt es sich bei den gewählten Optionen um für den aktuellen Teilnehmer- oder Bankstatus ungültige EBICS-Transaktionen, erfolgt eine Warnmeldung. So ist z. B. im Teilnehmerstatus "Neu" eine Schlüsseländerung eine ungültige Transaktion. Ein gültiger Status für eine solche Transaktion wäre z. B. der Status "Bereit". Aktuelle sowie gültige **Zustände von Teilnehmer- bzw. Bankseite** werden hier zu Ihrer Information eingeblendet.



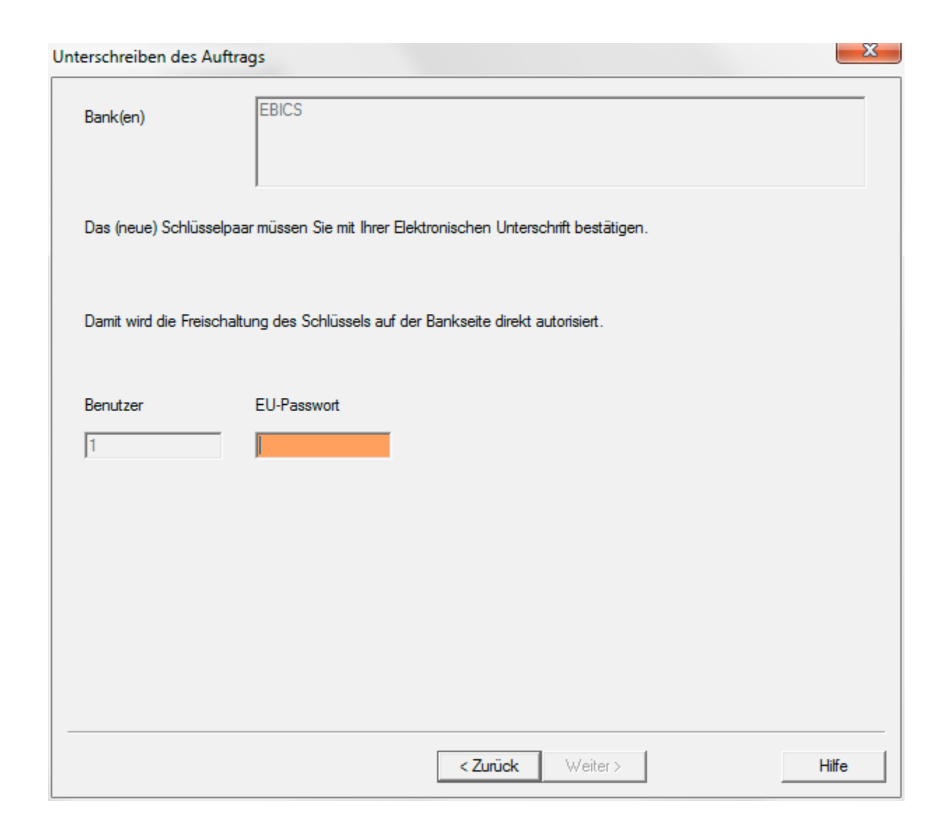


Beachten Sie bitte:
Sie sollten mit dem Assistenten im Falle dieser Warnmeldung nur fortfahren, wenn Sie sich absolut sicher sind, dass der Status in der Bankparameterdatei nicht korrekt ist. Andernfalls wird die Kommunikation mit der Bank nicht erfolgreich sein und Ihr Zugang ist dann nicht mehr möglich.

Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].

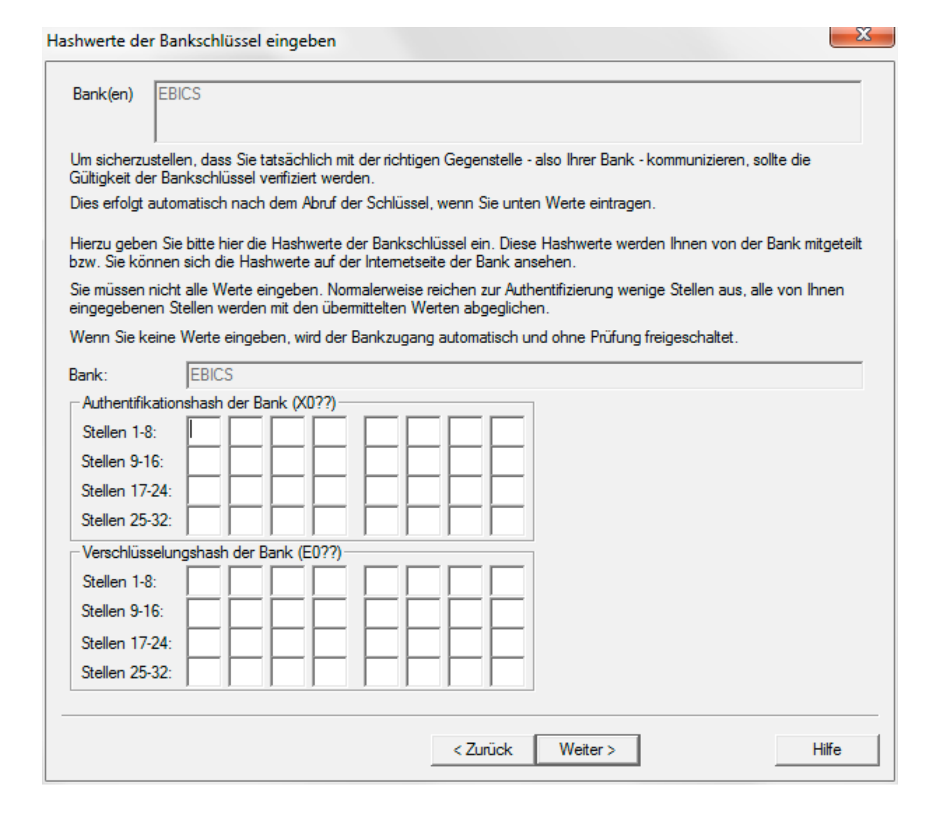
4 **Unterschreiben des Auftrags** (nicht bei der ausschließlichen Erstellung von HPB-Aufträgen)
Im Anschluss muss das (neue) Schlüsselpaar mit Ihrer Elektronischer Unterschrift betätigt werden, damit die Freischaltung des Schlüssels auf der Bankseite sofort autorisiert ist.
Um nachfolgend die Elektronische Unterschrift leisten zu können, werden Sie aufgefordert, Ihr **EU-Passwort** einzugeben.





Danach drücken Sie die Schaltfläche [***Weiter >***].

Falls ein HPB-Abruf durchgeführt werden soll, werden anschließend die Hashwerte der Bankschlüssel für die automatische Verifikation nach deren Abruf abgefragt (Diese Seite wird je ausgewählter Bank angezeigt.).



Bestätigen Sie anschließend mit [***Weiter >***].

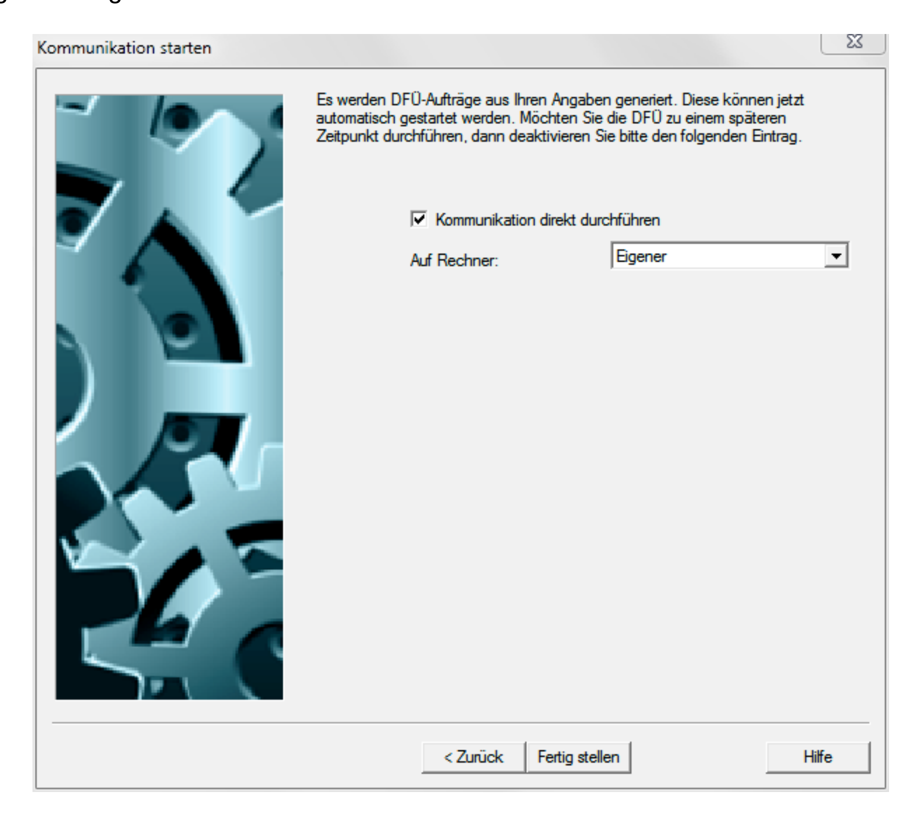


5 **Kommunikation starten**

Es wird ein Kommunikationsauftrag/werden Kommunikationsaufträge (HCA und ggf. HPB) aus Ihren Angaben generiert. Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".

Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.

Über die Schaltfläche [***< Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.



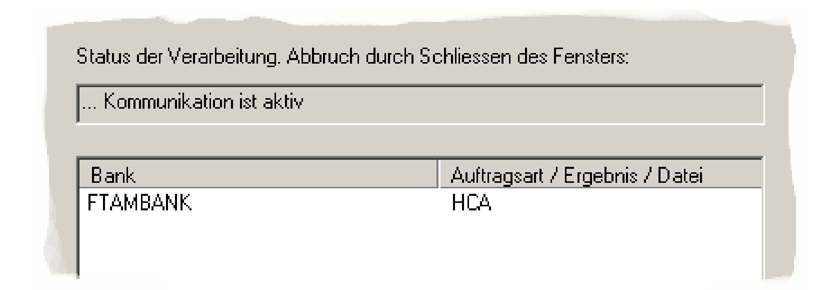
Da Aufträge zum Schlüsselversand mit einer Unterschrift versehen werden müssen, erfolgt im Anschluss an das Drücken der Schaltfläche [***Fertig stellen***] die Aufforderung zur Eingabe des EU-Mediums. (Das EU-Passwort wurde ja bereits eingegeben: Schritt **4**)

Nach Einlegen des EU-Mediums und Bestätigen mit [***OK***] wird in Abhängigkeit von dem oben erwähnten Kontrollkästchen die Kommunikation sofort oder später (d. h. aus dem Datei-Manager heraus) gestartet.

Im unterem Teil des Fensters erscheint dann eine Anzeige zum Status der Verarbeitung.



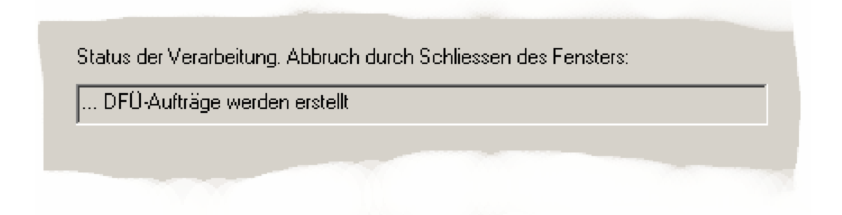
Kommunikation sofort:



Nach dem erfolgreichen Übertragen schließen Sie das erscheinende Hinweisfenster mit [***OK***].

Den Assistenten schließen Sie über ein abschließendes Drücken der Schaltfläche [***Fertig stellen***].

Kommunikation später:



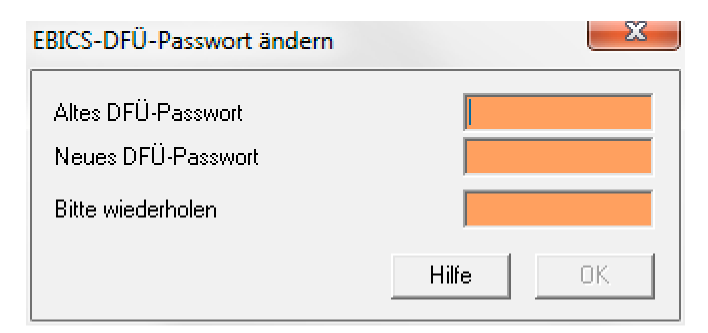
Das erscheinende Hinweisfenster bestätigen Sie mit [***OK***]. Bearbeiten Sie die Kommunikationsaufträge mit dem entsprechenden Ordnungsbegriff anschließend im Datei-Manager weiter.



4.8 EBICS-DFÜ-Passwort ändern

Sollte sich die Notwendigkeit einer Änderung des DFÜ-Passwortes für Ihren EBICS-Zugang (d. h. des Zugriffspasswortes für die A- und V-Keys) ergeben, so wählen Sie aus dem Menü -Kommunikation- den Menüpunkt -EBICS-DFÜ-Passwort ändern- aus.

Das Programm fordert Sie im ersten Schritt auf, das bisher verwendete **alte EBICS-Passwort** einzugeben. Im Anschluss geben Sie dann das **neue EBICS-Passwort** ein. Die Eingaben erfolgen verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt. Aus Sicherheitsgründen müssen Sie die Eingabe des neuen EBICS-Passwortes **bitte wiederholen**. Sie bestätigen Ihre Eingaben durch Anwahl der Schaltfläche [***OK***].



Eine abschließende Meldung bestätigen Sie ebenfalls mit [***OK***].



Analog zum Ändern des EU-Passwortes ist hierfür keine Kommunikation zur Bank notwendig.

Ist in der BPD-Datei für Sie definiert, dass das DFÜ-Passwort gespeichert werden soll, so wird das neue Passwort auch in der BPD-Datei geändert.

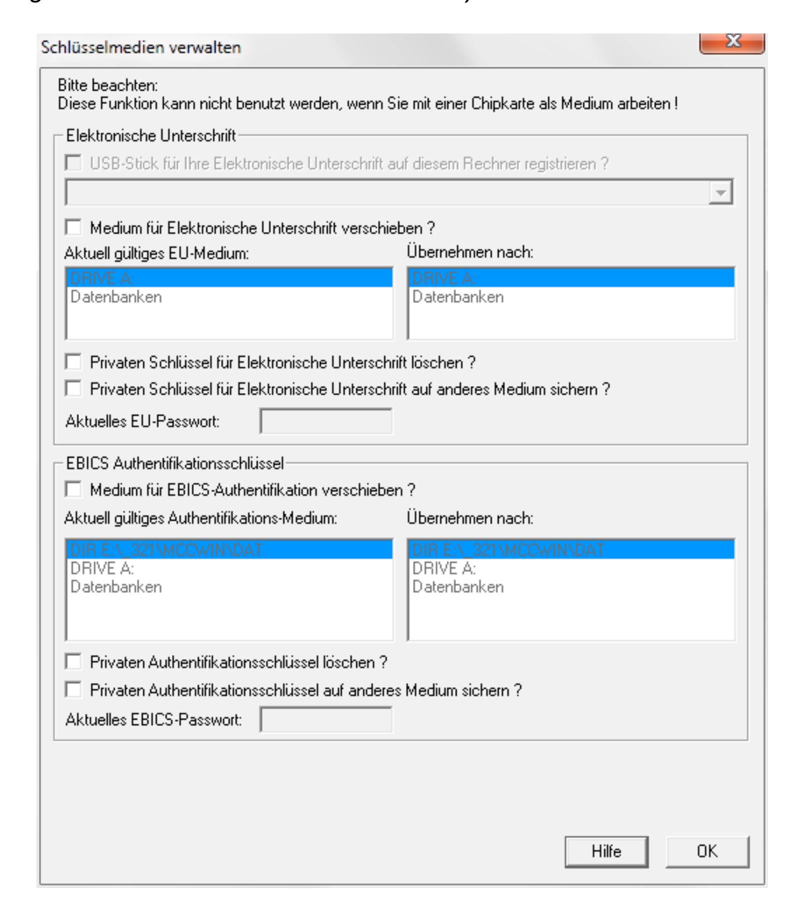


4.9 Assistent Schlüsselmedien verwalten

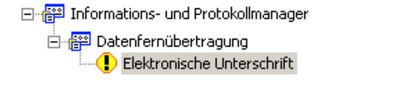
Beachten Sie bitte:
Diese Schlüsselmedienverwaltungsfunktion kann nicht genutzt werden, wenn Sie mit einer Chipkarte als Schlüsselmedium arbeiten.

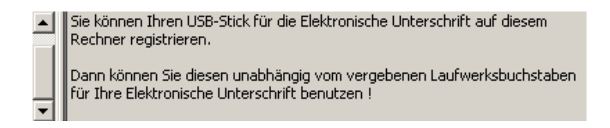
Sollen die privaten Schlüssel für die bankfachliche EU bzw. die privaten EBICS-Authentifikationsschlüssel auf externe Medien verlagert (z. B. nach Aktivieren des Parameters "**Externes Medium für EBICS-Authentifikationsschlüssel benutzen**") oder zwischen Schlüsselmedien verschoben werden, so verwenden Sie dazu den Assistenten "Schlüsselmedien verwalten". Außerdem können Sie hierüber Schlüssel löschen oder auf einem anderen Medium sichern.

Welche Medien, z. B. für die externe Schlüsselablage, genutzt werden können, ist abhängig von benutzerspezifischen (s. Kapitel 5.4.1: *Registerkarte Benutzer*) und rechnerspezifischen Einstellungen (s. Kapitel 6.1.5: *Registerkarte Elektronische Unterschrift*).



Benutzer, die mit USB-Sticks arbeiten, werden im IPM darauf hingewiesen, dass die Möglichkeit besteht, einen Stick registrieren zu lassen.

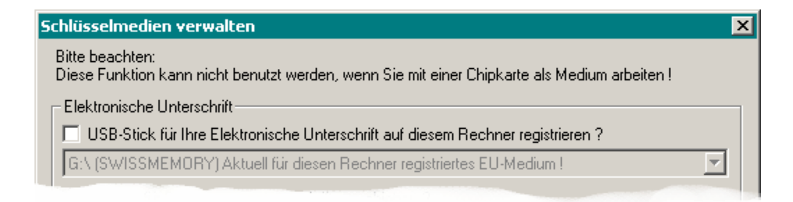




Zunächst haben Sie hier die Möglichkeit, einen bestimmten USB-Stick rechnerbezogen für die EU zu registrieren. Markieren Sie dazu das Kontrollkästchen "**USB-Stick für Ihre Elektronische Unterschrift auf diesem Rechner registrieren?**". Wählen Sie dann den gewünschten Stick über die Auswahlliste aus. Nach Bestätigen mit [***OK***] ist der gewählte Stick auf diesem Rechner registriert.



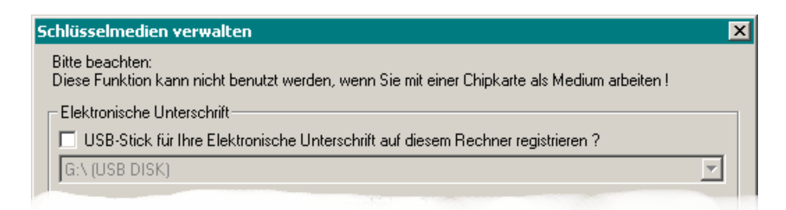
Anschließend wird ein Hinweis angezeigt, dass es sich bei dem gewählten Stick um das aktuell für diesen Rechner registrierte EU-Medium handelt.



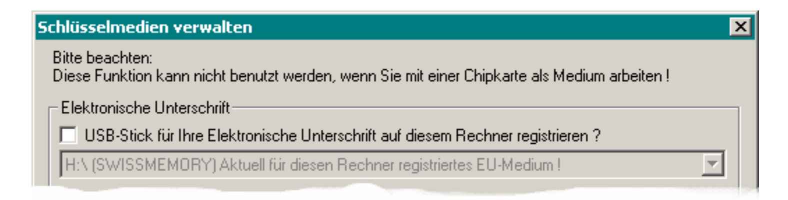
Dieser registrierte USB-Stick wird dann auf diesem Rechner **unabhänging vom benutzten Laufwerksbuchstaben** immer für die Elektronische Unterschrift benutzt.

Beispiel:

In diesem Fall ist das Laufwerk G:\ bereits durch einen anderen USB-Stick belegt.



Anhand des GUID des USB-Sticks wird der registrierte Stick (dem hier der Laufwerksbuchstabe H.\ zugewiesen wurde) vom System als das für die EU registrierte Medium eindeutig identifiziert.



Diese Einstellung muss für einen Benutzer ggf. auf weiteren Rechnern wiederholt werden, da die GUIDs rechnerspezifisch belegt werden. Ist für den Benutzer/Rechner kein USB-Stick registriert, wird die Laufwerkseinstellung aus den Systemparametern benutzt.

Der nächste Bereich des Assistenten ist grundsätzlich den Aktionen vorbehalten, die die **Elektronische Unterschrift** betreffen. Jede Aktion ist hier mit dem aktuell gültigen **EU-Passwort** zu autorisieren.

Für die bei **EBICS** außerdem nötigen **Authentifizierungsschlüssel** steht der untere Bereich des Assistenten zur Verfügung. Aktionen, die diese Schlüssel betreffen, sind mit dem aktuell gültigen **EBICS-Passwort** zu autorisieren.

Durch Markieren der entsprechenden Optionen im EU-, im EBICS- oder in beiden Bereichen entscheiden Sie, ob die Aktionen einzeln oder zeitgleich durchgeführt werden sollen.

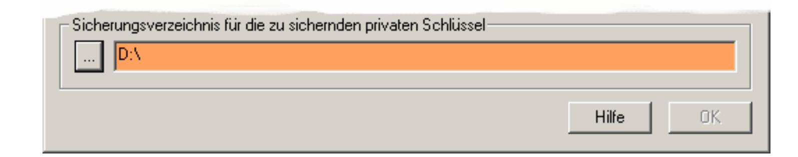
Die erste Option dient jeweils zum **Verschieben** des privaten Schlüssels für die bankfachliche EU bzw. des privaten EBICS-Authentifikationsschlüssels von dem aktuellen Medium auf ein neues Zielmedium. Wählen Sie dazu jeweils aus den verfügbaren Laufwerken auf der linken Seite das gerade verwendete Medium, auf der rechten Seite das gewünschte Zielmedium aus.



Nach Eingabe des EU- bzw. EBICS-Passwortes und Bestätigen mit [***OK***] wird/werden der/die Schlüssel auf das Zielmedium verschoben.

Die zweite Option dient jeweils zum **Löschen** des privaten Schlüssels für die bankfachliche EU bzw. des privaten EBICS-Authentifikationsschlüssels.
Nach Bestätigen mit [***OK***] wird/werden der/die Schlüssel gelöscht.

Die dritte Option dient jeweils zum **Sichern** des privaten Schlüssels für die bankfachliche EU bzw. des privaten EBICS-Authentifikationsschlüssels auf ein weiteres Medium. Nach Anwahl dieser Option öffnet sich ganz unten im Assistenten ein Feld, in das Sie, ggf. über die Ordnerauswahl mittels der Schaltfläche [**...**], das gewünschte Sicherungsverzeichnis eingeben.
Nach Eingabe des EU- bzw. EBICS-Passwortes und Bestätigen mit [***OK***] wird/werden der/die Schlüssel in das Sicherungsverzeichnis kopiert.





4.10 Zertifikate verwalten

Wenn Zugänge zur Webapplikation mit TLS-Verschlüsselung oder mit TLS-Verschlüsselung und Clientzertifikaten genutzt werden sollen, müssen vor der Konfiguration der Zugänge die jeweiligen Zertifikate über die Applikation generiert werden. Hierfür stehen die folgenden Menüpunkte zur Verfügung:

4.10.1 Systemschlüssel und Zertifikat erstellen
4.10.2 TLS-Schlüssel und Zertifikat erstellen

Was bei diesen in erster Linie für Systemadministratoren relevanten Funktionen im Einzelnen zu beachten ist, erfahren Sie im gesonderten Dokument "Schnelleinstieg für Systemadministratoren" in Kapitel: *Zugänge zur Webapplikation* (Datei *-QuickRef_Admin-*.PDF im ..\DOC-Verzeichnis der Installation).

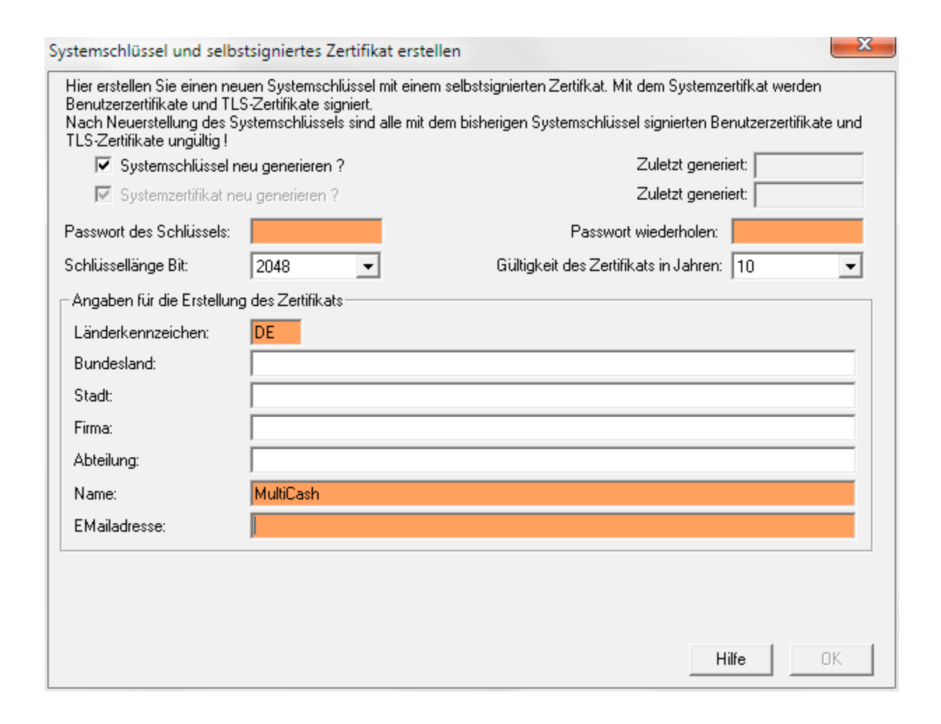


4.10.1 Systemschlüssel und Zertifikat erstellen

Über diesen Menüpunkt erstellen Sie einen neuen Systemschlüssel mit einen selbstsignierten Zertifikat. Mit dem Systemzertifikat werden Benutzerzertifikate und TLS-Zertifikate signiert.



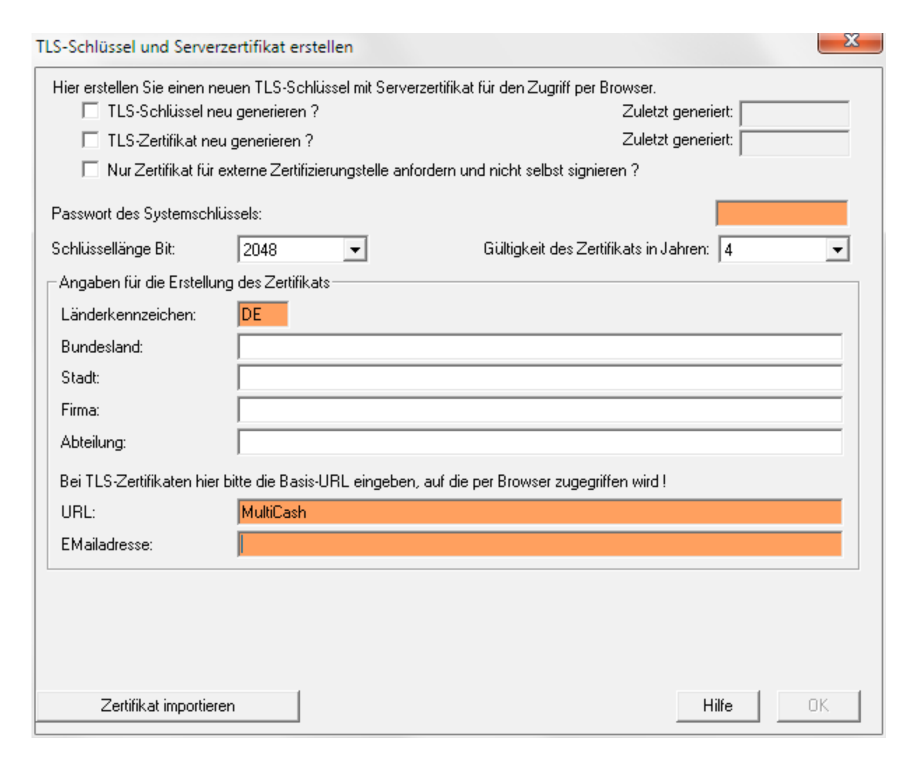
Nach Neuerstellung des Systemschlüssels sind alle mit dem bisherigen Systemschlüssel signierten Benutzerzertifikate und TLS-Zertifikate ungültig!





4.10.2 TLS-Schlüssel und Zertifikat erstellen

Über diesen Menüpunkt erstellen Sie einen neuen TLS-Schlüssel mit Serverzertifikat für den Zugriff per Browser.



Hierbei existieren es zwei Varianten:

Variante 1: Selbstsigniertes Zertifikat

Wählen Sie hierzu die Optionen -TLS-Schlüssel neu generieren?- und -TLS-Zertifikat neu generieren?-. Nach Eingabe der erforderlichen Daten bestätigen Sie mit [***OK***].

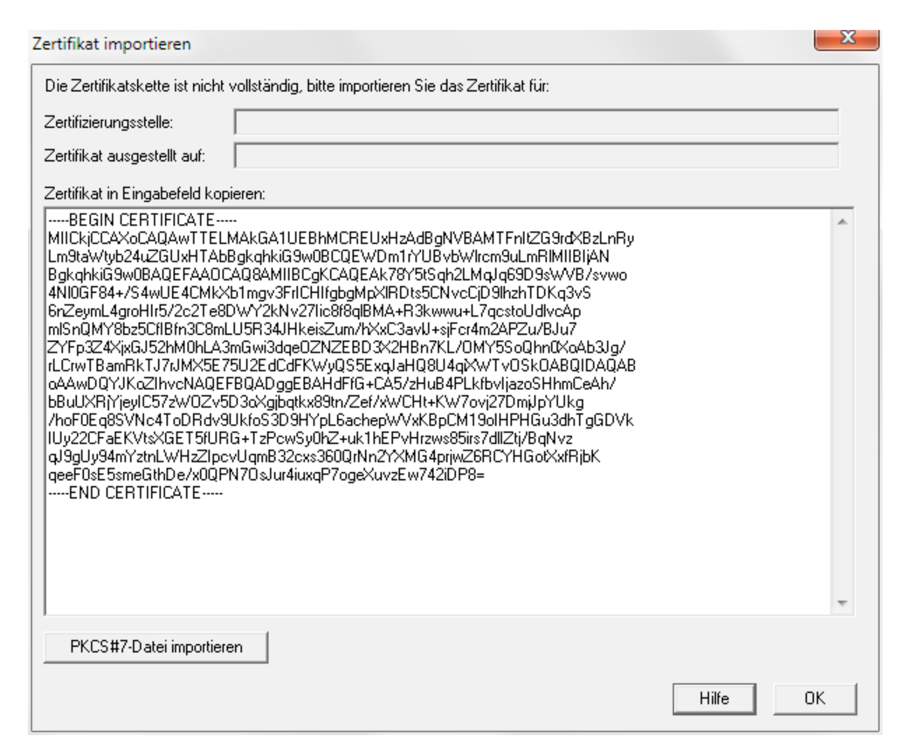
Variante 2: Zertifikat einer Zertifizierungsstelle

Markieren Sie hierfür die Kontrollkästchen -TLS-Schlüssel neu generieren?- und -Nur Zertifikat für externe Zertifizierungstelle anfordern und nicht selbst signieren?-.

Nach Eingabe der erforderlichen Daten und Bestätigen mit [***OK***] wird ein Zertifikatsrequest generiert, der von Ihnen an die Zertifizierungsstelle übermittelt werden muss. Durch diese erhalten Sie dann später einen Zertifikatsresponse.

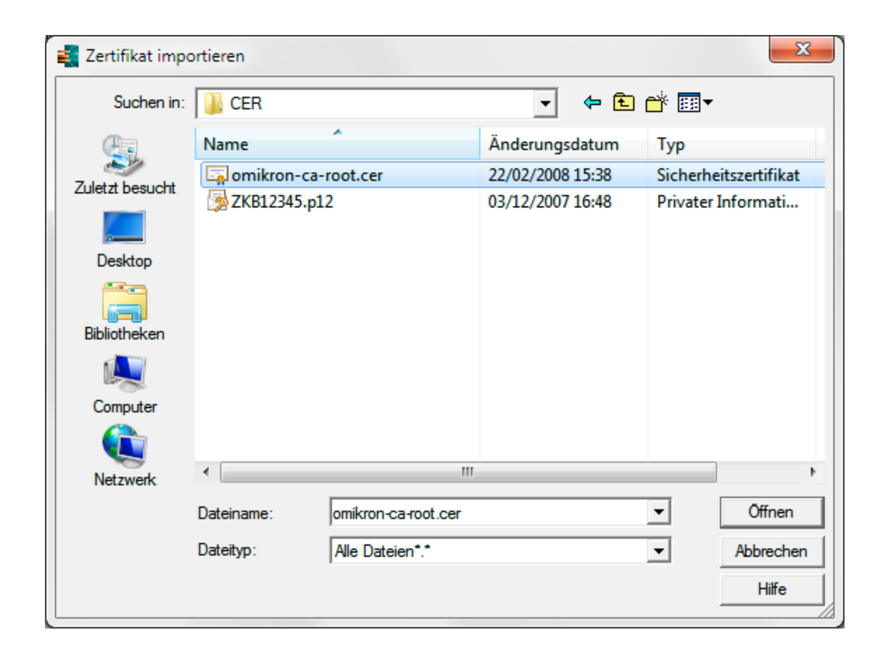


Um das angeforderte Zertifikat in das System zu übernehmen, klicken Sie zunächst auf die Schaltfläche [***Zertifikat importieren***]. Fügen Sie anschließend den zuvor kopierten Zertifikatsresponse in das große Eingabefeld ein und bestätigen dann mit [***OK***].

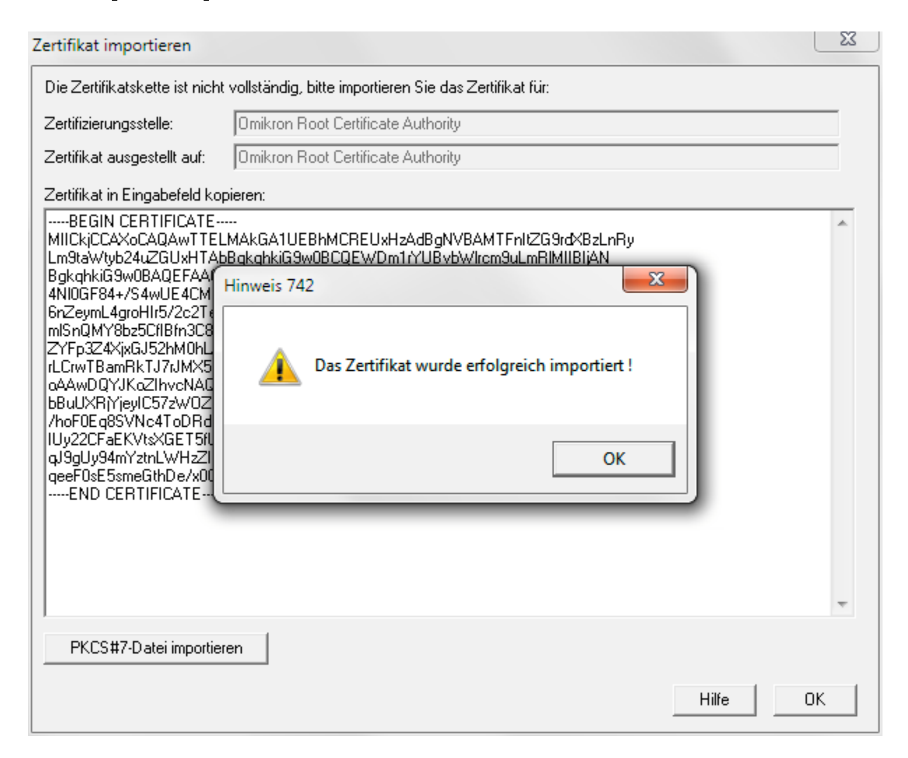


Alternativ können Sie entsprechende Zertifikatsdateien über die Schaltfläche [***PKCS#7-Datei importieren***] aus anderen Verzeichnissen in das System übernehmen. Anschließend öffnet sich das übliche Fenster zur Auswahl der Dateien.





Über die Schaltfläche [***Öffnen***] können Sie die Zertifikatsdatei übernehmen.



Ist der Import erfolgreich, bekommen Sie unter "**Zertifizierungsstelle**" angezeigt, von wem das Zertifikat ausgestellt worden ist. Unter "**Zertifikat ausgestellt auf**" werden Ihnen ebenfalls die gültigen Informationen angezeigt.



4.10.3 Zertifikat anfordern

Die weiteren Menüpunkte stehen nur dann zur Verfügung, wenn das Zusatzmodul "Zertifikatsverwaltung" installiert wurde.

Dies sind:

4.10.3 *Zertifikat anfordern*
4.10.4 *Zertifikat importieren / installieren*
4.10.5 *Zertifikat zuordnen*

Nach Aufruf des Menüpunktes -Zertifikat anfordern- werden Sie zunächst aufgefordert, das entsprechende EU-Medium einzulegen.

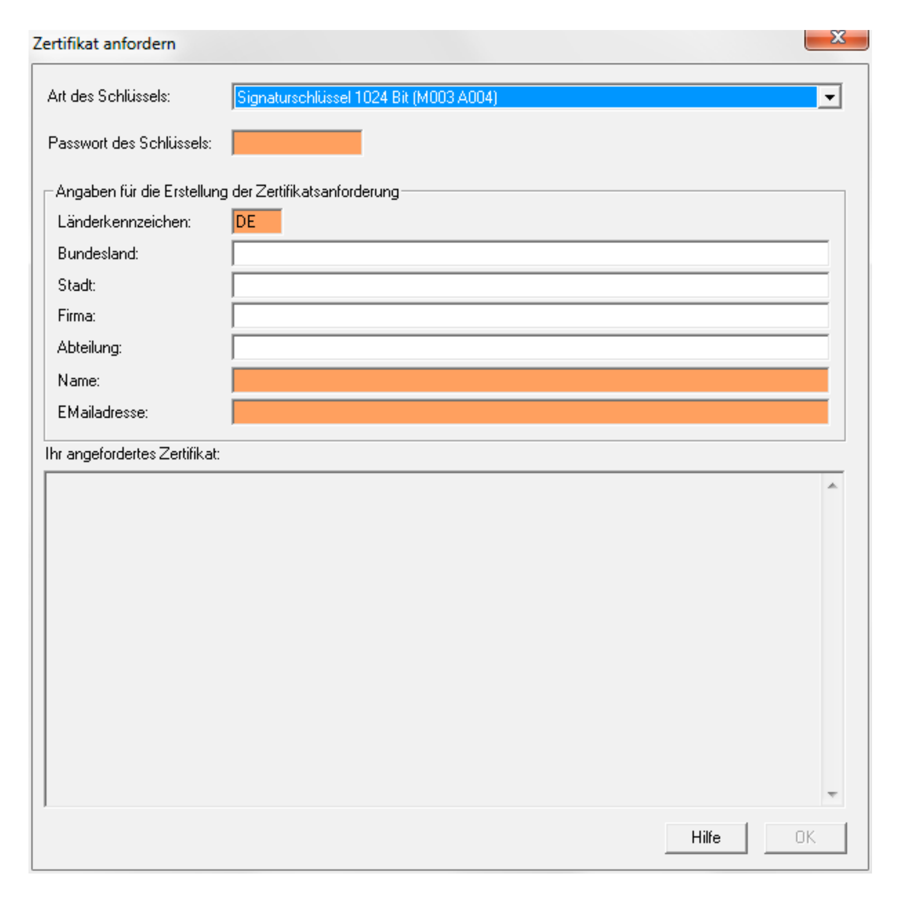
Im folgenden Dialog sind dann einige für die Erstellung der Zertifikatsanforderung notwendige Angaben zu machen:

Art des Schlüssels

Passwort des Schlüssels

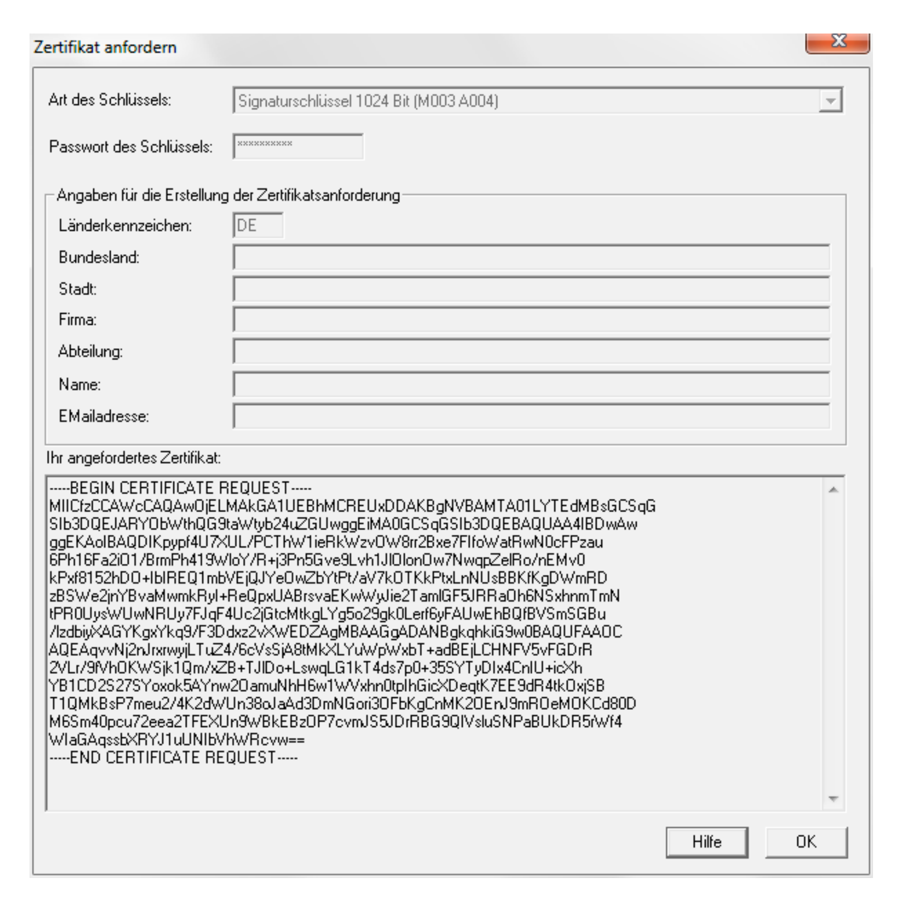
Um den Zugriff auf den Schlüssel zu ermöglichen, muss das EU-Passwort eingegeben werden.

Weitere Pflichtangaben müssen in den Feldern **Länderkennzeichen**, **Name** und **E-Mailadresse** zu machen. Optional sind die Felder **Bundesland**, **Stadt**, **Firma** und **Abteilung** zu befüllen.





Nach Drücken der Schaltfläche [***OK***] erscheint das angeforderte Zertikat im großen Feld unterhalb der Angaben.



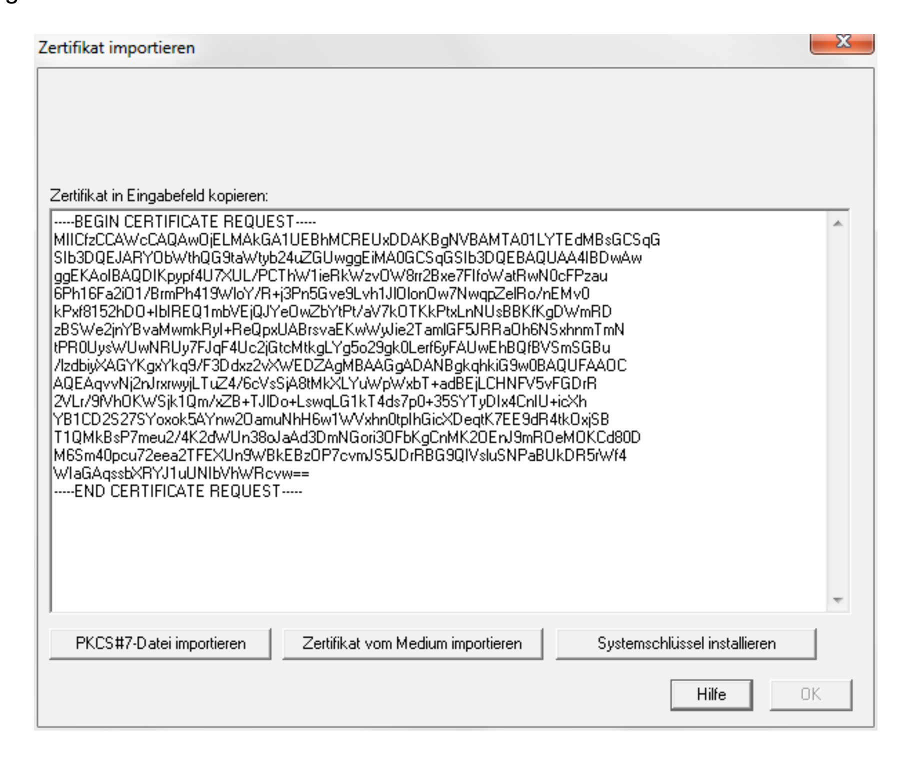


4.10.4 Zertifikat importieren

Um das angeforderte Zertifikat in das System zu übernehmen, fügen Sie das zuvor kopierte Zertifikat in das große Eingabefeld ein und bestätigen dann mit [***OK***].

Über die Schaltfläche [***PKCS#7-Datei importieren***] können Sie entsprechende Zertifikatsdateien aus anderen Verzeichnissen in das System übernehmen. Anschließend öffnet sich das übliche Fenster zur Auswahl der Dateien.

Über die Schaltfläche [***Zertifikat vom Medium importieren***] können Sie eine Zertifikatsdatei direkt von einem Signaturmedium übernehmen.



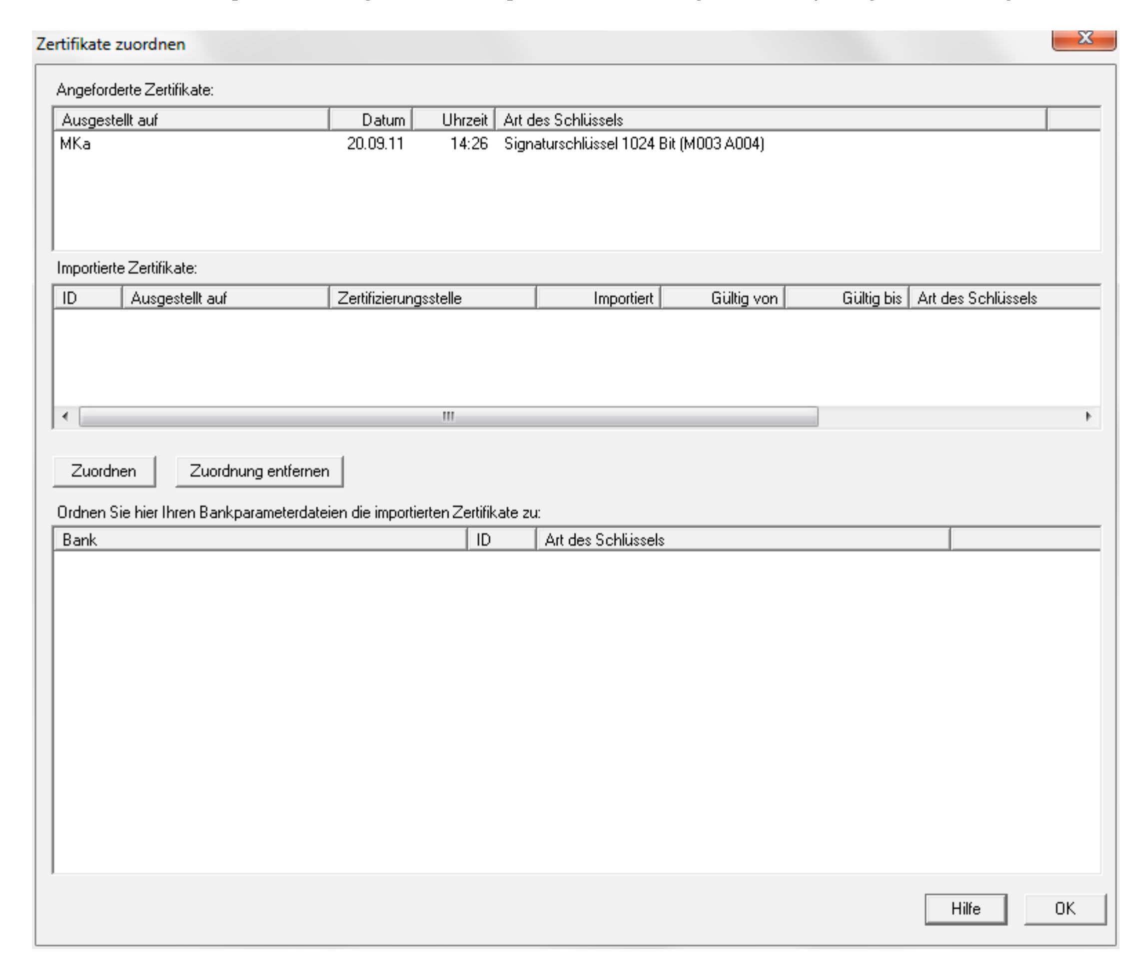


4.10.5 Zertifikat zuordnen

Mittels dieses Dialogs werden die angeforderten oder importierten Zertifikate den jeweiligen Banken (d. h. Bankparameterdateien), die die Verwendung von Zertifikaten unterstützen, zugeordnet.

In den Anzeigefeldern können passende Einträge ausgewählt und dann über die Schaltfläche [***Zuordnen***] miteinander verknüpft werden.

Über die Schaltfläche [***Zuordnung entfernen***] können derartige Verknüpfungen wieder gelöst werden.





Inhaltsverzeichnis: Kapitel 5

Seite



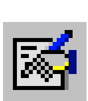
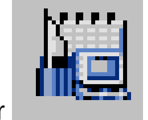
5 Datei-Manager / Ausführen der DFÜ

Der Datei-Manager ist das zentrale Steuerung- und Kontrollinstrument der Kommunikation des Programms, d. h. für alle ein- und ausgehenden Dateien, Nachrichten etc.
Zum Ausführen der DFÜ stehen Ihnen die Funktionsschaltflächen im Datei-Manager (Kap. 5.1) bzw. die unter "DFÜ ausführen" (Kap. 5.3) beschriebenen Funktionen zur Verfügung.

5.1 Datei-Manager

Den Datei-Manager erreichen Sie über

das Icon

 oder 

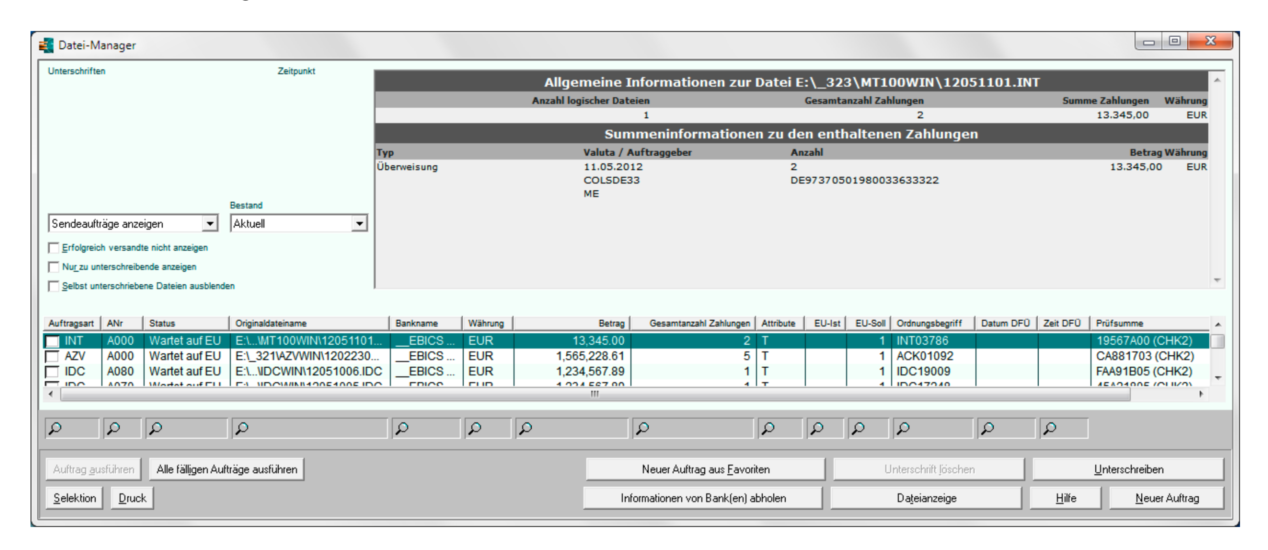
oder

den Menüpunkt -Kommunikation- / -Datei-Manager-.

Die Steuerung der Kommunikation erfolgt ausschließlich über den Datei-Manager.
Der Datei-Manager zeigt alle Informationen über ein- und ausgehende Bank-Transaktionen an. Anwender, die das System häufig nutzen, haben hier die Kontrolle über alle anstehenden und ausgeführten DFÜ-Aufträge und steuern ganz zentral die Vergabe von Unterschriften und den Versand der Dateien. Alle Informationen für Referenzzwecke und über den Verlauf der Bearbeitung laufen hier zusammen.

5.1.1 Datenbankübersicht Datei-Manager

Nach Aufruf des Datei-Managers gelangen Sie zunächst in eine Datenbankübersicht, in der Sie die per DFÜ ein- und ausgehenden Dateien verwalten.

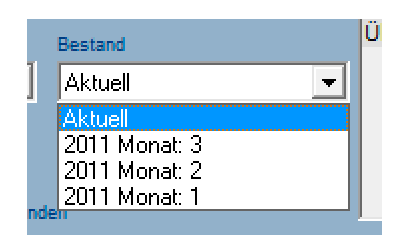


Im **Anzeigebereich** der Datenbankübersicht werden Ihnen (bis zu sechs) geleistete **Unterschriften** mit Datum und Uhrzeit (**Zeitpunkt**) der Unterschrift angezeigt, daneben in Kurzform der Dateiinhalt. Wurde die interne Freigabefunktion aktiviert (s. Parameter "Anzahl interner Freigaben" im Basismodul-Kapitel 6.1.5: *Elektronische Unterschrift / Dateimanager*), werden die Kennungen der Personen, die die **Freigaben** erteilt haben (bis zu zwei mit Datum/Uhrzeit), angezeigt. Ein Unterzeichner kann dann prüfen, wer die Freigabe vorgenommen hat.

Über eine Auswahlliste können Sie die Anzeige auf bestimmte Gruppen von DFÜ-Aufträgen beschränken. So haben Sie die Wahl zwischen:
- **Sendeaufträge anzeigen**
- **Abholaufträge anzeigen**
- **Empfangene Dateien anzeigen** und
- **Alle anzeigen**.

Durch Markieren des Kontrollkästchens "**Erfolgreich versandte nicht anzeigen**" schließen Sie die erfolgreich per DFÜ übertragenen Dateien (Status "OK") von der Anzeige aus.
Über das Kontrollkästchen "**Nur zu unterschreibende anzeigen**" können Sie die Ansicht auf die noch mit einer Elektronischen Unterschrift zu versehenden Dateien (Status "Wartet auf EU") eingrenzen.
Mittels des Kontrollkästchens "**Selbst unterschriebene Dateien ausblenden**" können Sie die von Ihnen als angemeldetem Benutzer unterschriebenen Dateien ausblenden.

Über die Auswahlliste "**Bestand**" können Sie neben den aktuellen Auftragsdaten auch historische Bestände anzeigen, sofern die Dateimanagerhistorie über den Parameter "**Historie pflegen?**" (vgl. Basismodul-Kapitel 6.1.5: *Elektronische Unterschrift / Dateimanager*) aktiviert wurde. Funktionen wie [***Selektion***] oder [***Druck***] wirken immer nur auf den gerade ausgewählten Bestand.



In der **Datensatzliste** der Datenbankübersicht sind die einzelnen Einträge anhand der Auftragsart (Sessiontyp), der Auftragsnummer, des Auftragsattributes (vgl. z. B. DFÜ-Kapitel 1.2.3: *FTAM*), Ist- und Soll-Anzahl der Unterschriften, des Status (z. B. Abholen OK, Wartet auf DFÜ (EU), OK, fehlerhaft, abgelehnt, gelöscht, EU-Prüfung OK, EU fehlerhaft, DFÜ initiiert, Wartet auf DFÜ-PIN, Freigabe offen), des Dateinamens (einschließlich Laufwerks- und Pfadangabe, eines Ordnungsbegriffs (interner Name), das Datums und der Uhrzeit der DFÜ, des Namens der bei der DFÜ genutzten Bankparameterdatei (als Klartext falls vorhanden) sowie die Summe der Aufträge (Währung und Betrag) aufgelistet. Darüber könne die einzelnen Einträge besser identifiziert werden. Die Summe wird in Originalwährung angezeigt, wenn alle Aufträge die gleiche Währung haben. Bei Aufträgen in verschiedenen Währungen wird in die Basiswährung (also die Währung, die mit Kurs 1 in der Währungstabelle steht) umgerechnet und dann aufaddiert.
Die Spalte "Ordnungsbegriff" kann sehr einfach für eine selektierte Abarbeitung der DFÜ-Aufträge genutzt werden (früher DAD-Name).

Die Anzeige des **nächsten** Ausführungstermins in den Spalten "Datum DFÜ" und "Zeit DFÜ" der Übersicht (bei Kommunikationsaufträgen mit regelmäßigen Wiederholungsrhythmen) erfolgt immer dann, wenn der Status des Auftrages auf "DFÜ initiiert" steht und daher ein nächster Ausführungstermin existiert. Dann hat hier die Anzeige des nächsten Termins Vorrang vor der Anzeige des Zeitpunktes der letzten Ausführung (vgl. im nachfolgenden Beispiel Zeile 1).

Auftragsart	Status	Dateiname	Bankname	Ordnungsbegriff	Datum DFÜ	Zeit DFÜ
STA	DFÜ initiiert Eigener	C:\...\MCCWIN\BWMDA0L1.STA	Mandant 100	MANUELL	13.06.06	16:47
PTK	Wartet auf DFÜ Eigener	C:\...\MCCWIN\BWMDA020.PTK	Mandant 100	MANUELL		
STA	Fehlerhaft	C:\...\MCCWIN\BWMDA0K1.STA (11,0) Die Übertragung wurde ...	Mandant 100		13.06.06	15:42

Bei den Stati "Wartet auf EU/Wartet auf DFÜ/Abgelehnt/Gelöscht/Wartet auf DFÜ-PIN" bleibt die Zeitanzeige in der Übersicht leer (vgl. Zeile 2 des obigen Beispiels).
Bei den Stati "OK/Fehlerhaft/EU-Prüfung OK/EU fehlerhaft" wird der **letzte** Ausführungszeitpunkt angezeigt (vgl. Zeile 3 des obigen Beispiels).

Die **neueste Datei** (der aktuellste Kommunikationsauftrag) steht in der Liste jeweils **ganz oben**.

Mehrfachauswahl

Haben Sie in der Datenbankübersicht des Dateimanagers mehrere DFÜ-Aufträge durch Markieren der **Kontrollkästchen vor der Auftragsart** markiert, können bestimmte Funktionen in einer "Stapelverarbeitung" ausgeführt werden (sämtliche Aufträge markieren Sie über den Kontextmenüeintrag -Alle Sätze markieren-).
Dies erleichtert vor allem das Unterschreiben, da in diesem Fall nur einmal das EU-Passwort eingegeben werden muss.

Bei den Funktionen, mit denen diese Verarbeitung möglich ist, handelt es sich zum einen um die folgenden Menüpunkte aus dem Kontextmenü (rechte Maustaste):
- -Satz löschen-
- -Ablehnen-
- -Zurücksetzen-
- -Reaktivieren-

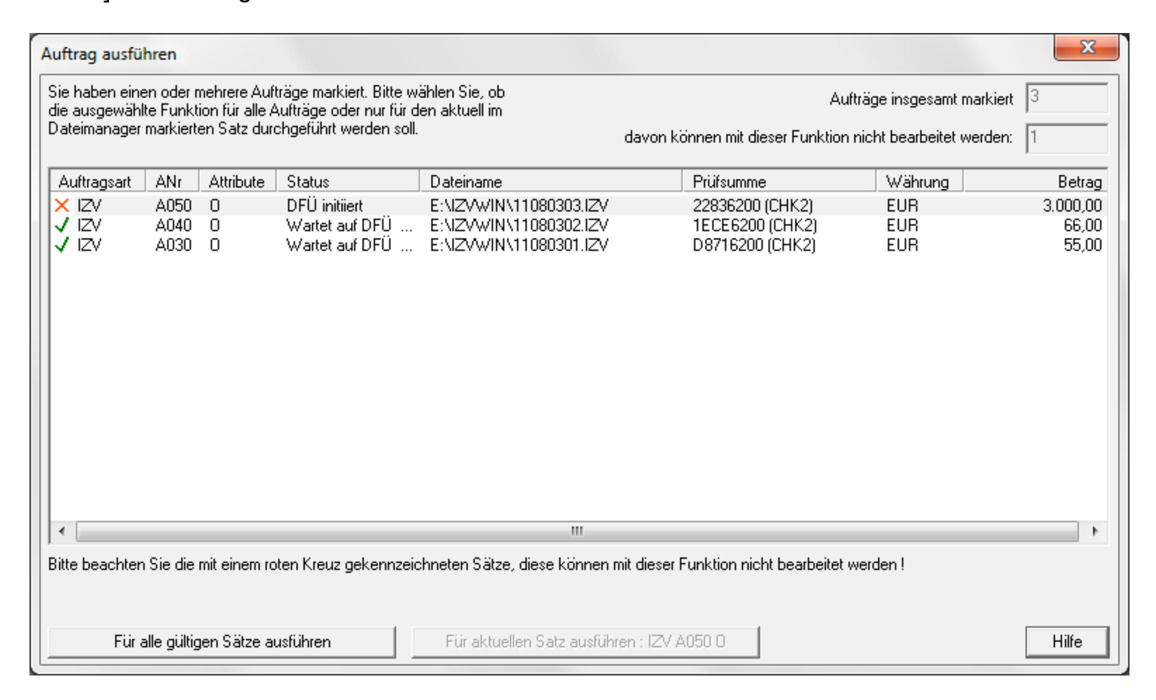
sowie um die folgenden Schaltflächen aus dem Funktionsbereich:
- [***Auftrag ausführen***]
- [***Unterschrift löschen***]
- [***Unterschreiben***].

Sind mehrere Datensätze im Dateimanager markiert, öffnet sich nach Anwahl einer der oben aufgeführten Funktionen ein weiterer Dialog (in der Titelleiste wird jeweils die gewählte Funktion angezeigt). Die im Dateimanager mit einem Haken versehenen Datensätze sind hier noch einmal aufgelistet.



Zusätzlich erhalten Sie über Symbole einen Hinweis, ob die gewählte Funktion auf den betreffenden DFÜ-Auftrag angewendet werden kann. Ein grüner Haken (✓) signalisiert, dass die gewählte Funktion auf den Datensatz anwendbar ist. Die mit einem roten Kreuz (✗) gekennzeichneten Datensätze dagegen können mit der gewählten Funktion nicht bearbeitet werden.

Beispiel:
So wurden im folgenden Fall drei DFÜ-Aufträge im Dateimanager markiert. Die Funktion [***Auftrag ausführen***] ist allerdings nur auf zwei der Datensätze anwendbar.

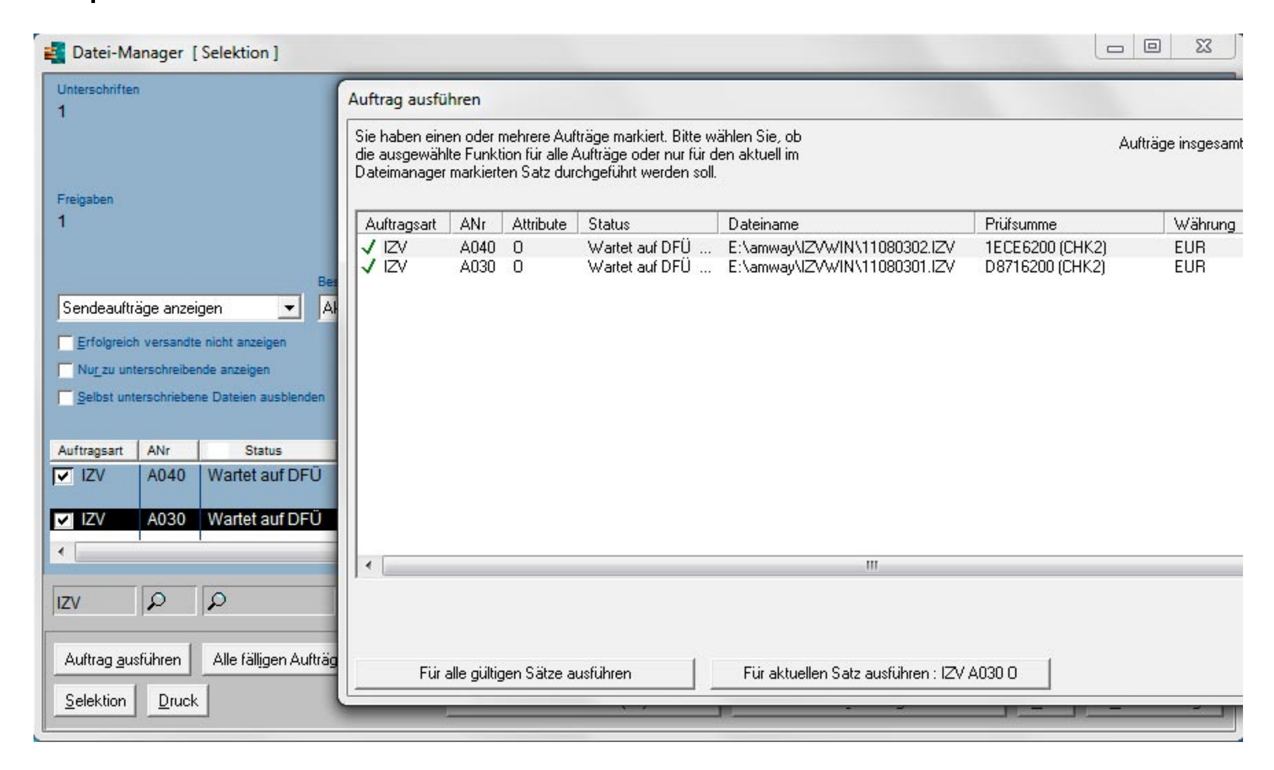


Die Anzahl der insgesamt im Dateimanager markierten Datensätze ist zu Ihrer Information rechts oben im Dialog angegeben. Darunter ist zusätzlich die Zahl der Datensätze angegeben, die mit der gewählten Funktion nicht bearbeitet werden können.

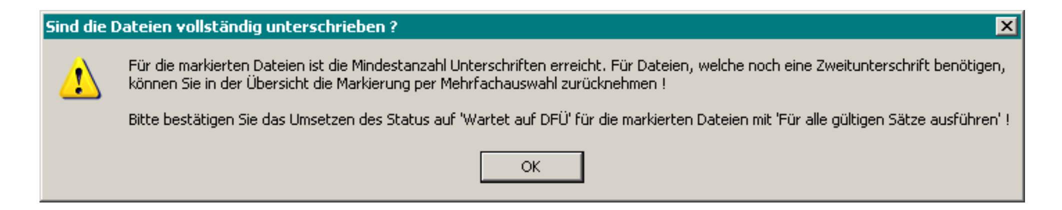
Sie können nun durch Anwahl der Schaltfläche [***Für alle gültigen Sätze ausführen***] entscheiden, ob die gewählte Funktion auf die möglichen (d. h. mit einem grünen Haken markierten) Datensätze angewendet werden soll.
Wählen Sie die Schaltfläche [***Für aktuellen Satz ausführen: <Kennung>***], wird die gewählte Funktion nur auf den im Dateimanager (!) hervorgehobenen Datensatz angewandt. Dies muss nicht notwendigerweise der im Mehrfachauswahl-Fenster hervorgehobene Datensatz sein. Zu eindeutigen Kennzeichnung wird zusätzlich die Kennung des im Dateimanager-Fenster hervorgehobenen Kommunikationsauftrages auf der Schaltfläche angezeigt. Dies ist z. B. im nachfolgenden Beispiel der Datensatz mit der Auftragsnummer A030, nicht der im Auswahl-Fenster hervorgehobene Satz mit der Auftragsnummer A040.



Beispiel:



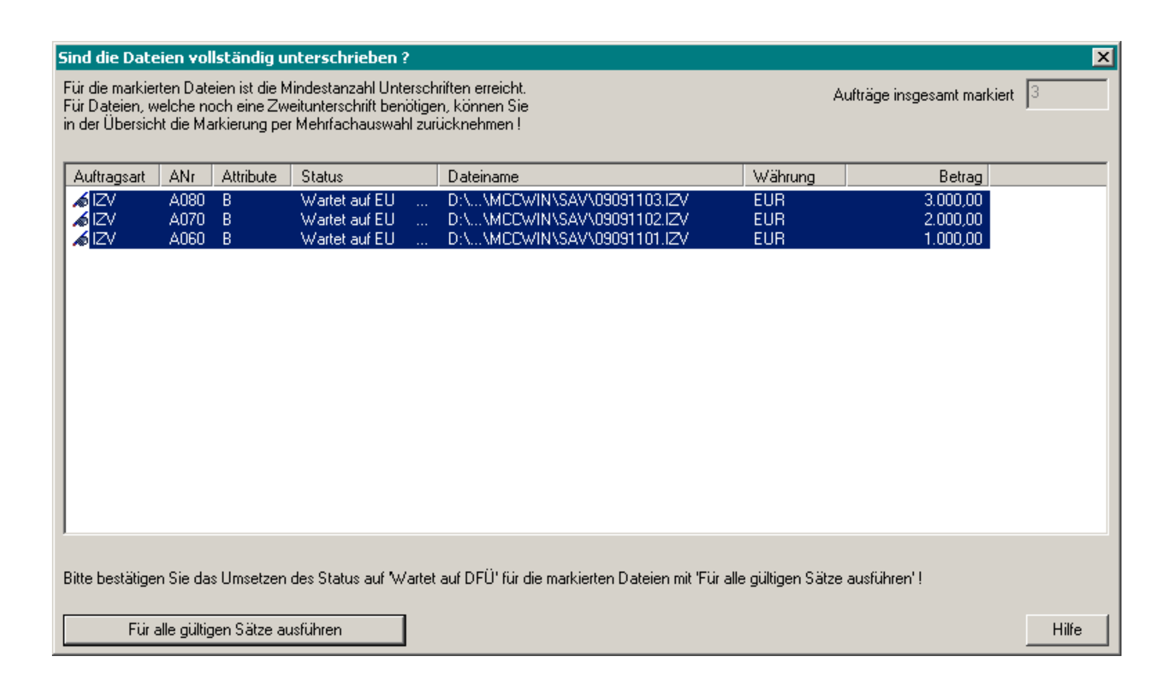
Nutzen Sie die Stapelverarbeitung für das **Unterschreiben von Dateien**, so schließen sich einmalig Abfragen nach dem EU-Medium sowie zur Eingabe des EU-Passwortes an.
Wird mit der geleisteten Unterschrift die Mindestanzahl an Unterschriften (abhängig von der Auftragsart) erreicht, erfolgt eine Abfrage, ob die Datei vollständig unterschrieben ist, sofern der entsprechende Systemparameter "**Abfrage, ob Unterschriften vollständig sind**" gesetzt ist (s. Kapitel 6.1.5: *Registerkarte Elektronische Unterschrift*).



Schließen Sie zunächst dieses Hinweisfenster mit [***OK***].

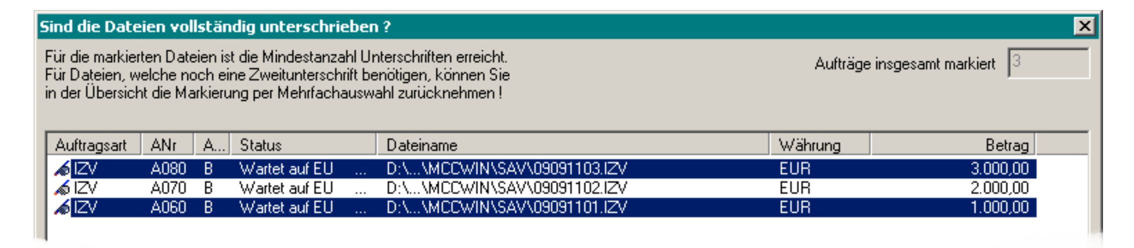
In dem nun textlich etwas veränderten Dialog sind die Dateien, bei denen das Unterschrifts-Soll erreicht wurde, bereits markiert (durch -in der Regel- graue Hinterlegung der Datensätze).





Durch Drücken der Schaltfläche [***Für alle gültigen Sätze ausführen***] würden alle derart markierten Dateien als vollständig unterschrieben gekennzeichnet und im Dateimanager zur Ausführung freigegeben (Status "Wartet auf DFÜ").

Sollen für einige der Dateien weitere Unterschriften geleistet werden, müssen Sie deren Markierung zurücknehmen.
Dies geschieht dadurch, dass Sie die vollständig unterschriebenen Dateien explizit durch Anklicken markieren (-in der Regel- blaue Cursormarkierung; ggf. Mehrfachauswahl bei gedrückter Shift- bzw. Ctrl-Taste). Nur für diese derart markierten Datensätze findet die Umsetzung des Status nach Drücken der oben genannten Schaltfläche statt.



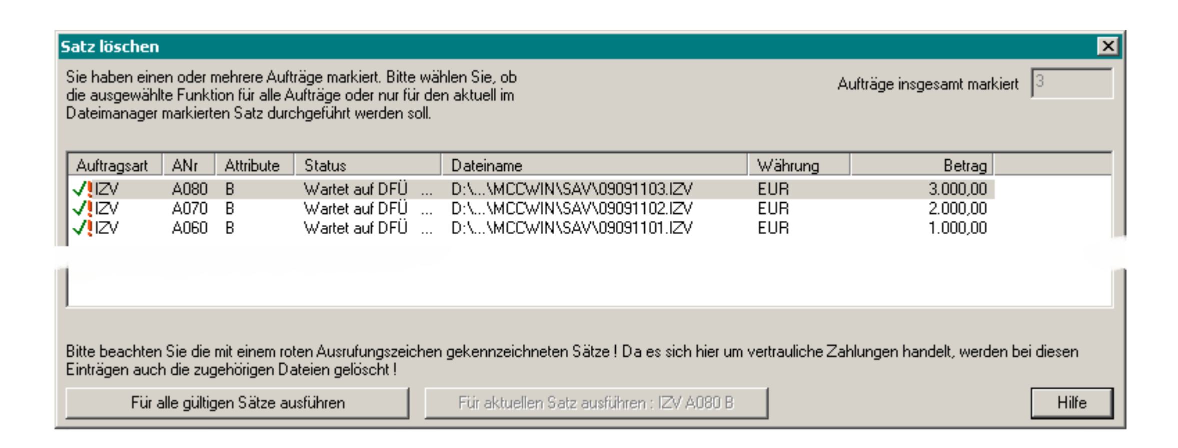
Zur Rücknahme sämtlicher Markierungen -d. h. es sollen für alle Dateien weitere Unterschriften geleistet werden- klicken Sie in den Weißraum unterhalb der Datensätze.

Bei den nicht markierten Datensätzen bleibt nach Verlassen des Dialogs über die oben genannte Schaltfläche der Status "Wartet auf EU" im Dateimanager erhalten. Für diese Dateien können dann erneut Unterschriften (Zweit- und weitere Unterschriften) geleistet werden (ggf. wiederum unter Nutzung der Mehrfachauswahl).

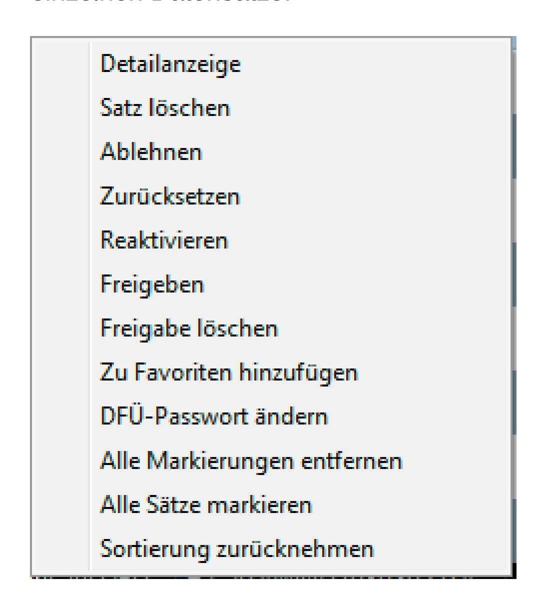
☞ **Bitte beachten Sie beim Löschen mittels Mehrfachauswahl:**

Während beim Löschen von Dateimanagereinträgen von normalen Aufträgen die Originaldateien bis zum Ablauf der sogenannten Verwahrdauer (vgl. Basismodul-Kapitel 6.4.1) erhalten bleiben, werden bei vertraulichen Zahlungen (d. h. Zahlungen mit gesetzter Zugriffsklasse) die Originaldateien aus Sicherheitsgründen sofort gelöscht. Um ein unabsichtliches Löschen von Zahlungsverkehrsdateien mit vertraulichen Zahlungen möglichst zu verhindern, sind diese Dateien mit einem zusätzlichen Ausrufungszeichen (!) gekennzeichnet.





Über das **Kontextmenü** (rechte Maustaste) erreichen Sie wichtige Bearbeitungsfunktionen für die einzelnen Datensätze:



Eine detaillierte Ansicht der Daten zu einem einzelnen Datensatz erhalten Sie über den Menüpunkt -**Detailanzeige**-.

Über -**Satz löschen**- können Sie Einträge aus dem Datei-Manager entfernen. Vor dem Löschen erfolgt jeweils zur Sicherheit eine Abfrage, ob der Eintrag tatsächlich gelöscht werden soll. Erst wenn Sie diese Abfrage mit [***Ja***] bestätigen, wird die entsprechende Aktion ausgeführt.

Nach dem Löschen eines Eintrages erfolgt zusätzlich eine Abfrage, ob die zugrundeliegende Datei ebenfalls gelöscht werden soll.

Beantworten Sie die Abfrage mit [***Ja***], wird die Originaldatei endgültig gelöscht. Bei [***Nein***] bleibt diese Datei erhalten und kann ggf. mit einem neuen DFÜ-Auftrag versandt werden.

Dateien, deren Eintrag im Datei-Manager gelöscht wurde (1. Abfrage [***Ja***]), die aber hier nicht sofort gelöscht wurden (2. Abfrage [***Nein***]), werden nach Ablauf der sogenannten Verwahrdauer, die für jede Auftragsart (Sessiontyp, z. B. IZV) spezifisch festgelegt wurde (vgl. Basismodul-Kapitel 6.4.1), automatisch gelöscht.
Bei vertraulichen Zahlungen (d. h. Zahlungen mit gesetzter Zugriffsklasse) werden die Originaldateien sofort aus dem ..\SAV-Verzeichnis gelöscht.



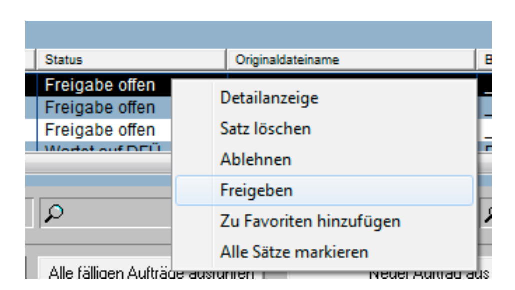
Über den Eintrag -**Ablehnen**- können Sie einen Auftrag auf den Status "Abgelehnt" setzen, d. h. von der DFÜ ausschließen. Damit diese Aktion ausgeführt wird, müssen sie vorher eine Sicherheitsabfrage mit [***Ja***] bestätigen.

Abgelehnte Aufträge können über den entsprechenden Kontextmenüeintrag wieder reaktiviert werden (s. u.).
Wird im Datei-Manager der Status einer Datei auf "gelöscht" oder "abgelehnt" gesetzt, werden die zu dieser Datei gehörigen Plandaten gelöscht.

Über den Eintrag -**Zurücksetzen**- können Sie einen Auftrag auf einen vorigen Status zurücksetzen. So können Sie z. B. einen Auftrag mit dem Status "DFÜ initiiert" über diesen Eintrag auf den Status "Wartet auf DFÜ" zurücksetzten. Auch hier erfolgt eine entsprechend zu beantwortende Sicherheitsabfrage.

Über den Eintrag -**Reaktivieren**- können Aufträge im Status "Abgelehnt" wieder aktiviert werden. EU-Aufträge werden dabei grundsätzlich auf den Status "Wartet auf EU" gesetzt, so dass diese nochmals mit einer Unterschrift bestätigt werden müssen.

Ist die interne Freigabefunktion aktiviert (s. Parameter "**Anzahl interner Freigaben**" im Basismodul-Kapitel 6.1.5: *Elektronische Unterschrift / Dateimanager*), erhalten in den Dateimanager eingestellte Dateien zunächst den Status "Freigabe offen". Autorisierte Mitarbeiter können über den Kontextmenüeintrag -**Freigeben**- die Freigabe durchführen.



Die Freigabe kann über den Kontextmenüeintrag -**Freigabe löschen**- wieder zurückgenommen werden.

Bevorzugte Auftragsarten (Sendeaufträge <u>und</u> Abholaufträge) können Sie über -**Zu Favoriten hinzufügen**- in die Liste Ihrer Favoriten aufnehmen.

Wurde eine Datei mit einem falschen DFÜ-Passwort versehen bzw. fehlt dieses, können Sie über den Kontextmenüpunkt -**DFÜ-Passwort ändern**- ein (neues) DFÜ-Passwort vergeben.
Geben Sie im anschließend erscheinenden Fenster das DFÜ-Passwort ein und bestätigen zur Ausführung mit [***OK***].

Bei fehlendem Passwort wird der Status danach von "Wartet auf DFÜ-PIN" auf "Wartet auf DFÜ" umgesetzt.
War der Auftrag vorher bereits fehlerhaft übertragen worden, dann wird der Status wieder auf "Wartet auf DFÜ" gesetzt. Der letzte Antwortcode (AC) wird auf 0 zurückgesetzt.

Über den Eintrag -**Erneut einstellen**- haben Sie die Möglichkeit, bereits erfolgreich versandte Aufträge aus dem Sicherungsverzeichnis nochmals einzustellen. Dazu wird die im ..\SAV-Verzeichnis liegende Originaldatei zunächst in ein darunterliegendes Verzeichnis ..\RESEND umkopiert und anschließend wird ein neuer DFÜ-Auftrag für diese Datei im Dateimanager aufgenommen.



Wurden zur Stapelverarbeitung mehrere oder alle Aufträge markiert, können über den Kontextmenüeintrag -**Alle Markierungen entfernen**- sämtliche Markierungen auf einmal entfernt werden.
Zum Markieren sämtlicher Datensätze verwenden sie den Kontextmenüeintrag -**Alle Sätze markieren**-.

Wurde durch Anklicken von Spalten eine Sortierung der Dateimanagerdaten vorgenommen, so kann diese über den Kontextmenüeintrag -**Sortierung zurücknehmen**- wieder entfernt werden.

<u>Funktionen im Zusammenhang mit speziellen Auftragsarten:</u>

Da für die Verwendung der Verteilten Elektronischen Unterschrift mit EBICS (s. Kapitel 1.2.5: *EBICS*) mehrere EBICS-Requests mit der bekannten Auftragsart **ESP** (Elektronische Zweitunterschrift senden) abgewickelt werden, existieren mehrere Funktionsaufrufe zu dieser Auftragsart, die an unterschiedlichen Stellen über den Datei-Manager aufgerufen werden.

So kann ein ESP-Auftrag über den Kontextmenüeintrag -**Originalauftrag bei der Bank stornieren**- storniert werden. Nach Auswahl des Eintrages muss der Stornoauftrag HVS (VEU-Storno) unterschrieben werden. Nach dem Versenden des Stornoauftrages ist keine Unterschrift mehr möglich. Es erfolgt daher ein Warnhinweis, dass die Datei unwiderruflich aus der VEU-Verarbeitung auf Bankseite entfernt wird, den Sie entsprechend mit [***Ja***] oder [***Nein***] beantworten.

Mit dem Ausführen des ESP-Auftrages erfolgt bis zu einer gewissen Dateigröße (in der Regel 1 MB, einstellbar) automatisch der Abruf der Originaldatei über den im Hintergrund ausgeführten EBICS-Request HVT (VEU-Transaktionsdetails abrufen). Wird bei Originaldateien, die diese Grenze überschreiten, versucht, Informationen über die Schaltfläche [***Dateianzeige***] anzeigen zu lassen, erfolgt ein Hinweis darauf, dass die Originaldatei noch nicht zur Verfügung steht, jedoch von der Bank abgeholt werden kann (mit einer Angabe der ungefähren Dateigröße). Beantworten Sie diesen Hinweis mit [***Ja***], wird ein entsprechender HVT-Abruf gestartet, um die Originaldatei abzuholen. Soll kein Abruf erfolgen, wählen Sie die Schaltfläche [***Nein***].

Im **Funktionsbereich** stehen Ihnen neben den Standardfunktionen [***Selektion***], [***Druck***] und [***Hilfe***] weitere Funktionen z. B. zum Versenden der Dateien und zum Leisten der Elektronischen Unterschrift zur Verfügung.

Durch Drücken der Schaltfläche [***Auftrag ausführen***] initiieren Sie für eine ausgewählte Datei die DFÜ und versenden die Datei.
Über die Schaltfläche [***Alle fälligen Aufträge ausführen***] starten Sie die Übertragung aller fälligen Kommunikationsaufträge, sofern der Status des Auftrags dies zulässt. Wurde zuvor eine Selektion durchgeführt, werden alle fälligen Aufträge versandt, die dieser Selektion entsprechen.

☞ **Bitte beachten Sie:**
Bei manuell auszuführenden Abholaufträgen ist die Schaltfläche [***Auftrag ausführen***] gesperrt und bei Verwendung der Schaltfläche [***Alle fälligen Aufträge ausführen***] werden diese Aufträge nicht berücksichtigt. Diese Aufträge können nur über das Icon "Informationen von Bank(en) abholen" ausgeführt werden (s. Kapitel 5.2). Um diese Aufträge besonders kenntlich zu machen, werden Sie in der Übersicht das Dateimanagers mit der für deaktivierte Einträge in den Systemparametern festgelegten Farbe gekennzeichnet, nachfolgend z. B. grau:

	Eigener	
STA	Wartet auf DFÜ	MANUELL
	Eigener	
STA	Wartet auf DFÜ	MANUELL
	Eigener	

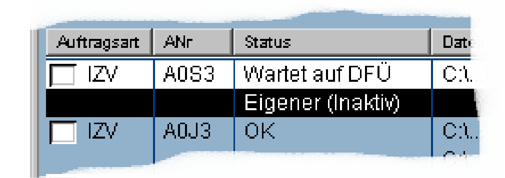


Nach Drücken der beiden Schaltflächen bzw. nach Auswahl der entsprechenden Schaltflächen im Mehrfachauswahl-Fenster öffnet sich **im Netzwerkbetrieb** unmittelbar vor der Ausführung zunächst eine Dialogbox, in der Sie den Rechner zur Ausführung der Kommunikationsaufträge bestimmen.

Sie haben die Wahl zwischen

- Nur fällige Aufträge des ausgewählten Rechners ausführen bzw.
- Alle fälligen Aufträge auf ausgewähltem Rechner ausführen,

verbunden jeweils mit der Auswahl des gewünschten **Rechnername**ns (bei Installation im Netzwerk) über eine Auswahlliste.
Die zuletzt gemachte Auswahl wird jeweils rechnerbezogen als Vorbelegung für die nächste Auswahl gespeichert. Rechner, auf denen die DFÜ-Leiste des Programms nicht geöffnet ist, sind in der Auswahlliste jeweils mit einem "(Inaktiv)" hinter dem Rechnernamen gekennzeichnet.
Zusätzlich wird der Name des Rechners für die DFÜ auch im Datei-Manager bei den Stati "Wartet auf DFÜ" bzw. "DFÜ initiiert" angezeigt, ebenfalls mit der Kennzeichnung "**(Inaktiv)**", falls auf diesem Rechner die DFÜ-Leiste des Programms nicht gestartet ist.



Als dritte Option steht

- Alle ausgewählten Aufträge wie im Auftrag definiert ausführen

zur Verfügung (bei Ausführung einzelner Kommunikationsaufträge ist nur diese Option vorhanden).

Mit Markieren der ersten Option "**Nur fällige Aufträge des ausgewählten Rechners ausführen**" bestimmen Sie, dass nur Kommunikationsaufträge, die zur Ausführung auf einem bestimmten Rechner definiert sind (z. B. auf dem eigenen), ausgeführt werden sollen.

Das Markieren der zweiten Option "**Alle fälligen Aufträge auf ausgewähltem Rechner ausführen**" bewirkt, dass **alle** fälligen Aufträge (z. B. von einer Arbeitsgruppe gesammelt) auf dem ausgewählten Rechner ausgeführt werden. Dies geschieht unabhängig davon, welcher Rechner für die DFÜ beim Anlegen des Kommunikationsauftrages eingestellt wurde.

Sollen sämtliche fälligen Aufträge so ausgeführt werden, wie es jeweils bei der Anlage des Kommunikationsauftrages definiert wurde, so wählen Sie die dritte Option: "**Alle ausgewählten Aufträge wie im Auftrag definiert ausführen**".

Nach Bestätigen mit [***OK***] werden die Kommunikationsaufträge entsprechend Ihrer Auswahl ausgeführt (Status wechselt auf "DFÜ initiiert").

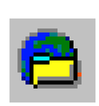
Die Schaltfläche [***Dateianzeige***] dient der Anzeige des vollständigen Dateiinhaltes in einem Display-Fenster. Die Präsentation der Informationen ist abhängig von der für die jeweilige Auftragsart hinterlegten Darstellungsart (mittels Parameter **Anzeigeform im Datei-Manager**; s. dazu Kapitel 6.4.1: *Registerkarte Auftragsarten*).

Mit Hilfe der Schaltfläche [***Unterschrift löschen***] können Sie eine bereits erteilte Elektronische Unterschrift wieder zurücknehmen.



Über die Schaltfläche [***Unterschreiben***] kann eine Originaldatei unterschrieben werden.

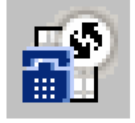
Mit der Schaltfläche [***Informationen von Bank(en) abholen***] können Sie Abholvorgänge bei (der) Bank(en) starten, wie Sie in Kapitel 5.2 beschrieben sind. Die Schaltfläche entspricht in ihrer Funktion der dort beschriebenen Schaltfläche für den Rundruf:

 oder .



Favorit ausführen

Über die Schaltfläche [***Neuer Auftrag aus Favoriten***] aus dem Datei-Manager heraus bzw. über den Menüpunkt -Kommunikation- / -DFÜ-Favorit ausführen- oder das Symbol

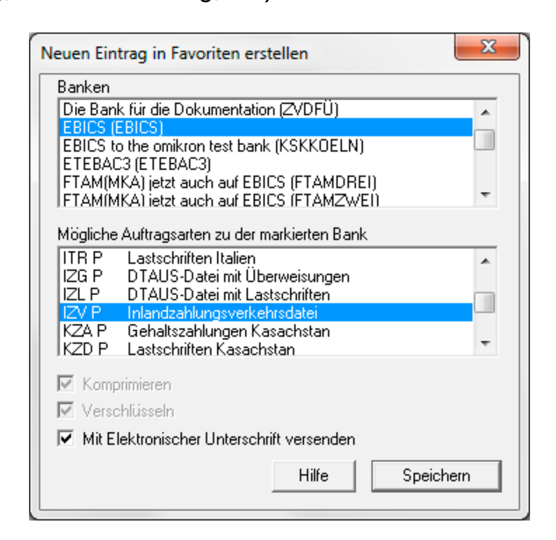
  oder 

können Sie eine Datenfernübertragung quasi per Mausklick durchführen, wenn Sie eine einfache und direkte Verbindung zu Ihrer "Haus-Bank" bevorzugen.
Der DFÜ-Favorit dient dabei zum Vordefinieren oft genutzter DFÜ-Aufträge (z. B. beim Versand von Fremddateien).
Durch Setzen des Parameters "**Planungsdaten generieren im Dateimanager**" (s. Kapitel 6.4.1: *Registerkarte Auftragsarten*) bei der entsprechenden Auftragsart wird automatisch die Plandatenerstellung auch beim Versand über den "Favoriten" ermöglicht.
Bei Sendeaufträgen wird eine Unterschrift bei der Auftragserstellung genutzt. Weitere Unterschriften können ggf. über den Datei-Manager geleistet werden.
Einen Auftrag fügen Sie in der Datenbankübersicht des Datei-Managers über das "Rechte-Maustasten-Menü" durch Anklicken des Eintrags -Zu Favoriten hinzufügen- zur Liste der bevorzugten Auftragsarten hinzu.

Nach Auswahl der Funktion "Favorit ausführen" (egal ob per Schaltfläche, Menüeintrag oder Symbol) zeigen Sie diese Auflistung an. Neben der Auftragsart und der favorisierten Bank wird dort anhand kleiner Symbole gekennzeichnet, ob die jeweilige Auftragsart mit ( ), mit Elektronischer Unterschrift ( ) und/oder mit ( ) durchgeführt wird.

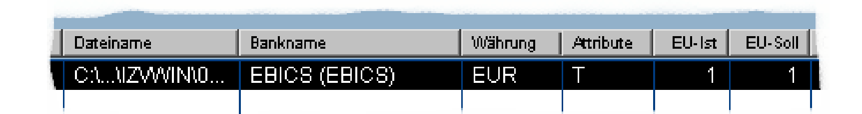
Sollten bereits Favoriten vorhanden sein, können Sie nicht mehr benötigte Favoriten über die Schaltfläche [***Eintrag aus Favoriten löschen***] wieder aus der Auflistung entfernen.

Über die Schaltfläche [***Neuen Eintrag in Favoriten erstellen***] können Sie an dieser Stelle einen Eintrag in den Favoriten vornehmen.
In der nachfolgenden Maske werden Ihnen die verfügbaren Banken angeboten, aus denen Sie Ihren Favorit auswählen. Darunter werden Ihnen die zu der markierten Bank möglichen Auftragsarten (inkl. Angaben zu Komprimierung, Verschlüsselung, EU).



Bei EBICS haben Sie die Möglichkeit, das Kontrollkästchen "Mit Elektronischer Unterschrift versenden" zu deaktivieren. Es werden dann Aufträge generiert, die nur mit einer Transportunterschrift versehen sind (Attribut T).





Dateiname	Bankname	Währung	Attribute	EU-Ist	EU-Soll
C:\...\IZVWIN\0...	EBICS (EBICS)	EUR	T	1	1

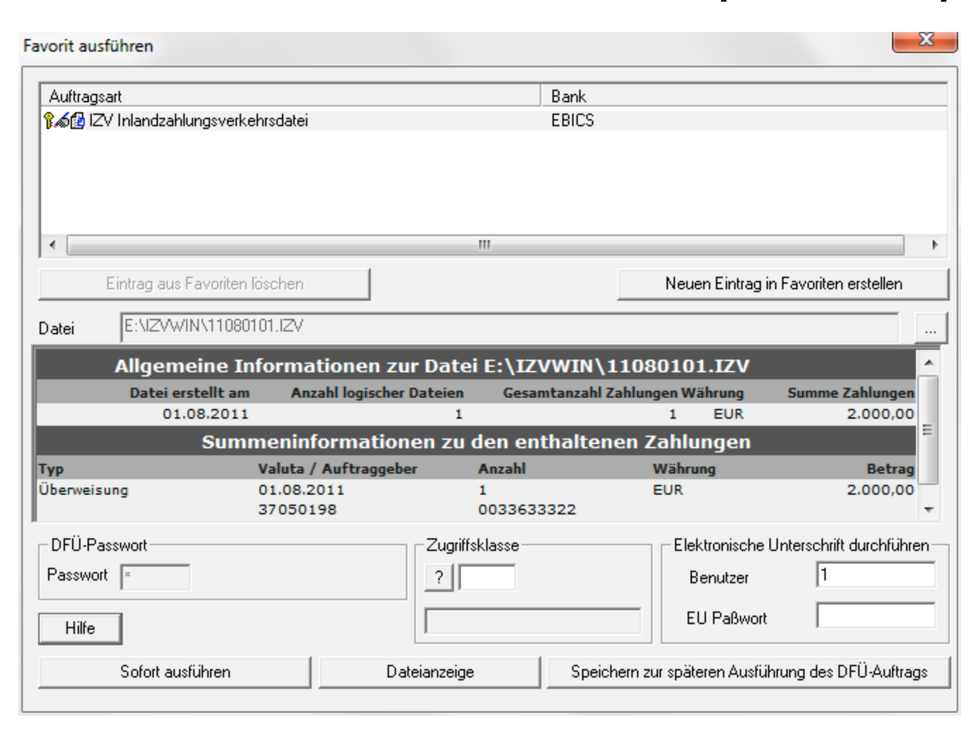
Bestätigen Sie Ihre Auswahl abschließend mit [***Speichern***].

Die zu versendende Datei wählen Sie hinter dem Feld "Datei" über die Schaltfläche [**...**] aus.
In Abhängigkeit von der gewählten Auftragsart wird direkt das passende Unterverzeichnis angeboten (z. B. bei IZV das Verzeichnis ..\IZVWIN). Nach der Auswahl können Sie unterhalb der Pfadangabe und der Anzeige des Dateiinhaltes das **DFÜ-Passwort** (ggf. ein zweites) und -falls gefordert- das zur Durchführung der Elektronischen Unterschrift notwendige **EU-Passwort** (das Feld "Benutzer" ist mit dem aktuellen Benutzer vorbelegt) eingeben.

Im Datei-Manager kann bei der Neuaufnahme im Favoriten eine **Zugriffsklasse** vergeben werden (vgl. Kapitel 7.8: *Hilfsdatenbank Zugriffsklassen*).

Die Schaltfläche [***Dateianzeige***] dient analog zur gleichnamigen Schaltfläche im Datei-Manager der Anzeige des vollständigen Dateiinhaltes der gewählten Datei.

Diesen definierten DFÜ-Auftrag können Sie über die Schaltfläche [***Speichern zur späteren Ausführung des DFÜ-Auftrages***] für ein späteres Versenden sichern. Diese Funktion nutzen Sie auch, wenn Sie weitere Unterschriften zum Auftrag im Dateimanager leisten möchten.
Sie können ihn aber auch direkt ausführen, indem Sie die Schaltfläche [***Sofort ausführen***] verwenden.



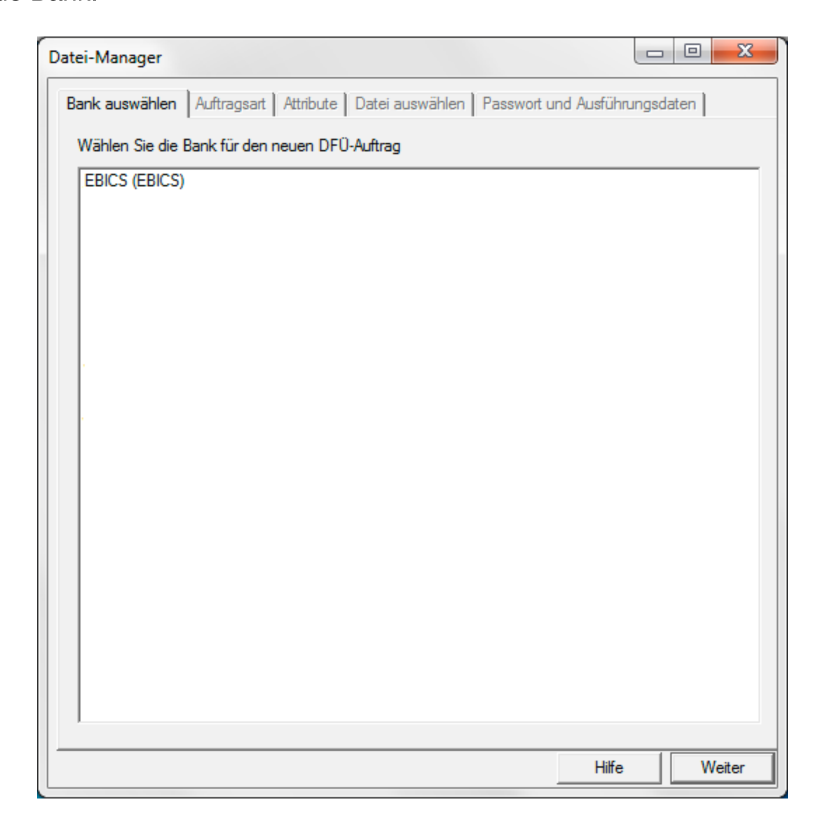
Über die Schaltfläche [***Neuer Auftrag***] schließlich nehmen Sie einen neuen DFÜ-Auftrag in den Datei-Manager auf.

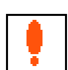
Registerkarte "Bank auswählen"

Im ersten Schritt müssen Sie festlegen, mit welcher Bank der im weiteren Verlauf zu erstellende DFÜ-Auftrag abgewickelt werden soll. Dazu werden auf der *Registerkarte "Bank auswählen"* in einer Auswahlliste alle im System gespeicherten BPDs mit ihrer aussagekräftigen Bezeichnung



angezeigt. Durch Anklicken mit der Maus bzw. durch Cursorpositionierung und selektieren Sie die betreffende Bank.





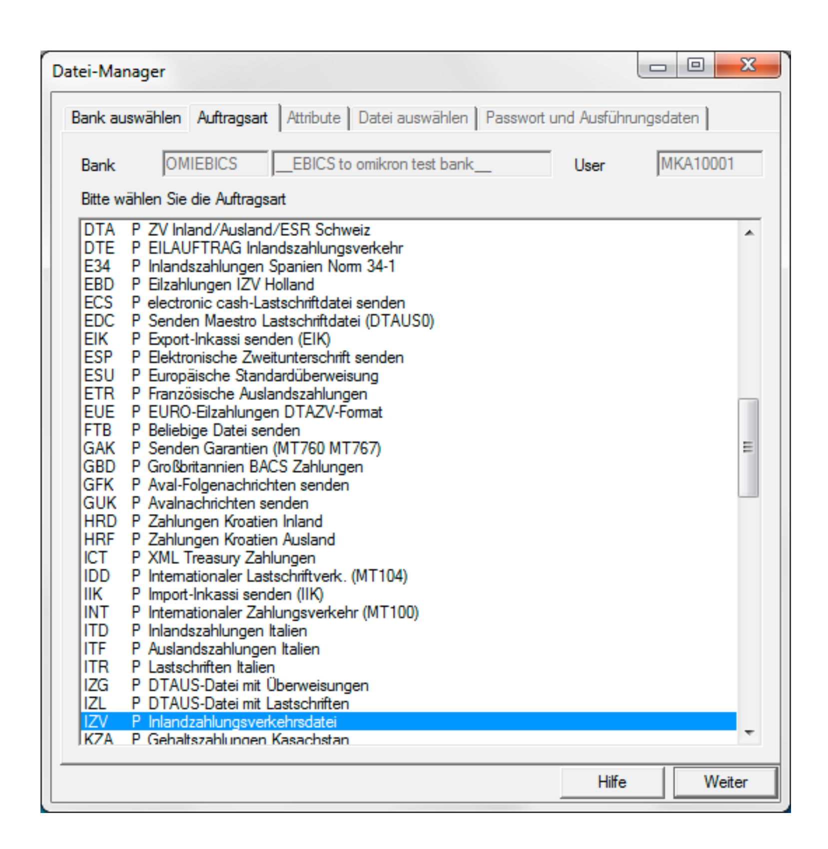
Ist unter -Verwaltung- / -Systemparameter- auf der *Registerkarte Programm* der Parameter "**ZVDFÜ-Bankparameterdateien auch von Diskette abfragen**" gesetzt, so fordert Sie das Programm zunächst auf, eine Diskette mit BPDs in das Diskettenlaufwerk einzulegen. Nach Bestätigung mit [***Ja***] sehen Sie in einem Auswahlfenster alle auf der Diskette vorhandenen BPDs und darüber hinaus auch die im Unterverzeichnis ..\DAT des Basismoduls gespeichert BPDs. BPDs auf der Diskette sind durch die Hintanstellung des Laufwerksbuchstaben gekennzeichnet. Bei Auswahl von [***Nein***] sehen Sie nur die im Unterverzeichnis ..\DAT des Basismoduls befindlichen Bankparameterdateien.

Anschließend legen Sie nach Drücken der Schaltfäche [***Weiter***] (damit wechseln Sie jeweils zur nach folgenden Registerkarte) die **Auftragsart** und bei Aufträgen unter Nutzung des DFÜ-Verfahrens FTAM auch die **Dateiart** fest:

Registerkarte Auftragsart

Abhängig von der im Datei-Manager gewählten Anzeigeoption (*Sendeaufträge anzeigen* etc.) werden auf der *Registerkarte Auftragsart* dementsprechend die jeweils aktivierten Auftragsarten (vgl. Basismodul, Kapitel 6.4: *Auftragsarten*) aufgelistet.





Auftragsarten sind z. B.

- IZV : Senden Inlandzahlungsverkehrsaufträge
- STA : Abholen Swift-Tagesauszüge
- PTK : Abholen Protokolle
- usw.

Sie wählen die Auftragsart durch einfaches Anklicken aus. Über Auftragsart wird auch das Format der zu sendenden oder abzuholenden Datei bestimmt, so dass im weiteren Programmverlauf entsprechende Prüfungen auf formale Richtigkeit der zu übertragenden Daten durchgeführt werden können.

Registerkarte Attribute

Die Auswahlliste zu den **Dateiart**en öffnen Sie durch Anklicken des nach unten weisenden Pfeils an der rechten Fensterseite.
Zur Eingabeerleichterung bei wiederholten Neuaufnahmen wird das Feld "Dateiart" in der Folge benutzerbezogen und je DFÜ-Verfahren mit der letzten hier gemachten Einstellung vorbelegt.

In der aktuellen Programmversion können Sie zwischen den folgenden Alternativen wählen:

- Orginaldatei ohne Unterschrift
- Originaldatei mit Unterschrift
- Unterschriftsdatei
- Original / Unterschrift zusammen
- Original / Verteilte Unterschrift
- Originaldatei mit Transportunterschrift

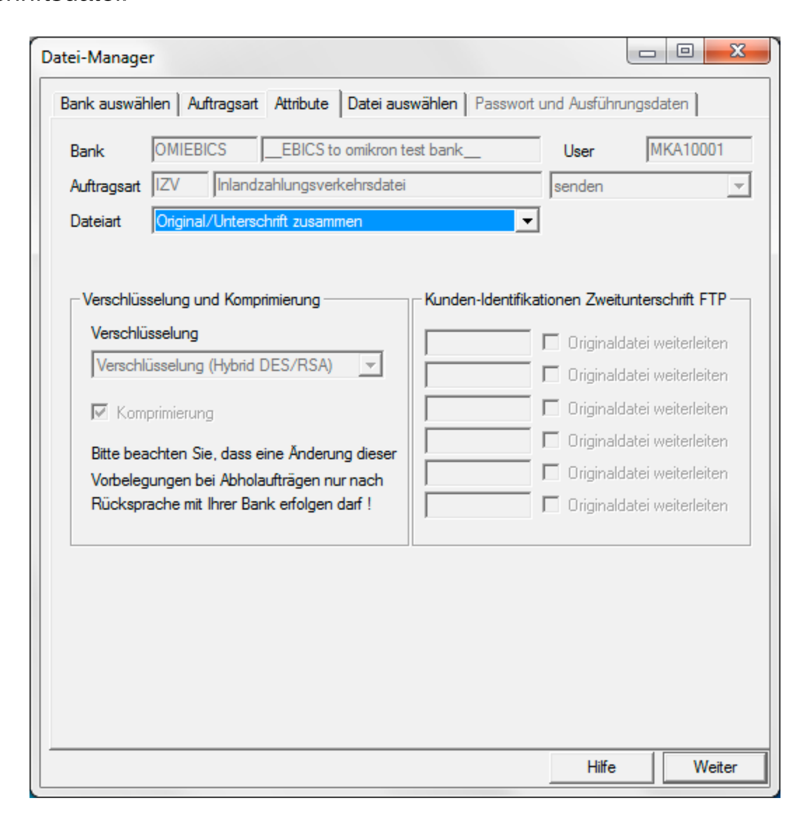
Wenn Sie das DFÜ-Verfahren MCFT nutzen und das Zusatzmodul EU installiert haben, können Sie zwischen den Dateiarten "Originaldatei mit Unterschrift" und "Originaldatei ohne Unterschrift" wählen. Informationen zur Elektronischen Unterschrift finden Sie in Kapitel 6: *Elektronische Unterschrift*. Weitere Angaben brauchen Sie nicht zu machen, da das Verfahren standardmäßig über Verschlüsselungs- und Komprimierungsmechanismen verfügt.

5.1.1 Datenbankübersicht Datei-Manager



Beim DFÜ-Verfahren FTAM haben Sie die Wahl zwischen den Dateiarten

- Orginaldatei ohne Unterschrift
- Originaldatei mit Unterschrift und
- Unterschriftsdatei.



Der Begriff **Originaldatei** bezieht sich auf die Datei, die Sie versenden bzw. abholen wollen. Die Originaldatei kann in einem bestimmten Format (DTAUS, DTAZV usw.) vorliegen, welches durch die Angabe der Auftragsart bestimmt wird. In Abhängigkeit der Auftragsart erfolgen Prüfungen auf formale Richtigkeit der zu übertragenden Daten.
Bei Übertragung von Zahlungsaufträgen mit dem DFÜ-Verfahren FTAM müssen Sie aus Sicherheitsgründen die **Elektronische Unterschrift** (= EU) einsetzen. Die Elektronische Unterschrift der Originaldatei kann direkt bei Erstellung des Zahlungsauftrages in einem Zahlungsverkehrsmodul geleistet werden. Die nachträgliche Unterzeichnung einer Originaldatei ist selbstverständlich auch möglich. Die Elektronische Unterschrift wird in einer **Unterschriftsdatei** abgelegt, die auch zu der den Auftrag ausführenden Bank übertragen werden muss.

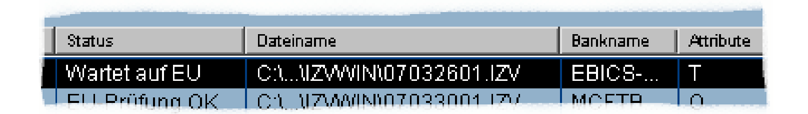
Wenn das Zusatzmodul FLAM installiert wurde, können Sie durch Markieren des Feldes "Komprimierung" eine effiziente Datenkomprimierung erreichen.

Beim DFÜ-Verfahren FTP haben Sie zusätzlich die Möglichkeit, die Kunden-Identifikationen einzugeben, die im Rahmen der Verteilten Elektronischen Unterschrift für eine Zweitunterschrift vorgesehen sind (Verteilerliste). Über ein Kontrollkästchen entscheiden Sie jeweils, ob die Originaldatei weitergeleitet werden soll oder nicht. Hierzu muss vorher die Dateiart "Original/Verteilte Unterschrift" ausgewählt werden.

Im Gegensatz zu FTAM bietet EBICS die Möglichkeit, die Unterschrift zusammen mit den Nutzdaten in einer Transaktion zu übermitteln und sofort das Ergebnis der Unterschriftsprüfung an den Kunden zu übermitteln. Für EBICS ist beim Vorbereiten eines Auftrages zum Versand mit Elektronischer Unterschrift also lediglich die Option **"Original/Unterschrift zusammen"** gültig. Wird eine andere, für EBICS nicht zulässige Option mit Unterschrift ausgewählt, wird automatisch auf die Option "Original/Unterschrift zusammen" umgestellt.

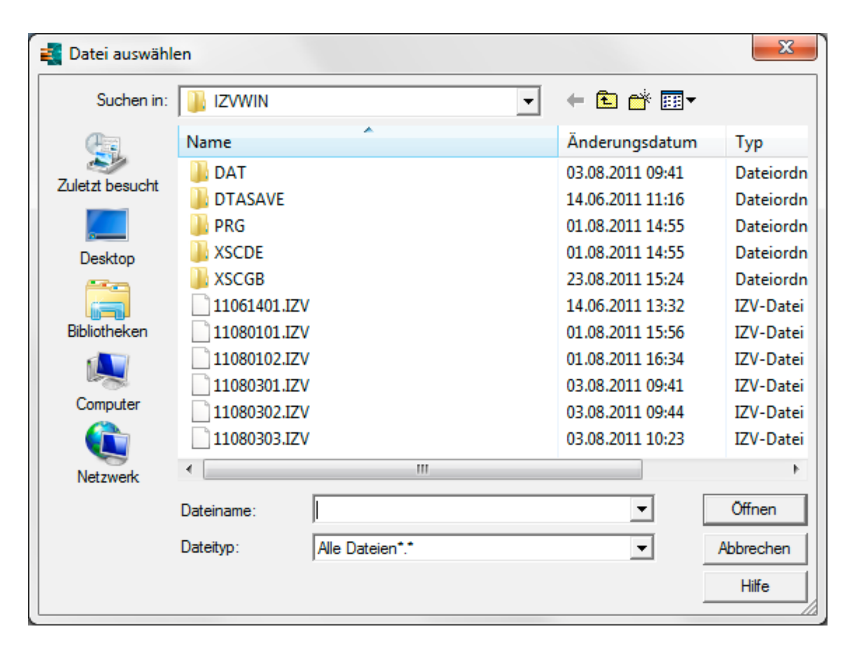


Gemäß EBICS-Spezifikation ist es auch möglich, eine Datei ohne bankfachliche Signatur zur Autorisierung mittels Begleitzettel zu versenden. Im Gegensatz zur Vorgehensweise bei FTAM oder FTP, wo die Datei ohne Unterschrift versandt werden kann, muss bei EBICS in diesem Fall die Datei jedoch immer mit einer Transportunterschrift versehen werden. Für diesen Fall steht bei der Neuaufnahme eines Kommunikationsauftrages die Option **"Originaldatei mit Transportunterschrift"** zur Verfügung. Wird die Option "Originaldatei ohne Unterschrift" ausgewählt, wird für EBICS automatisch auf "Originaldatei mit Transportunterschrift" umgestellt. Der Auftrag wird zur besseren Unterscheidung mit Attribut "**T**" und Status "Wartet auf EU" in den Datei-Manager eingestellt.



Registerkarte "Datei auswählen"

Bei Sendeaufträgen öffnet das Programm in Abhängigkeit von der gewählten Auftragsart das entsprechende Unterverzeichnis (z. B. bei Auftragsart IZV das Verzeichnis ..\IZVWIN), aus dem Sie die (Auftrags-)Dateien auswählen, die in den DFÜ-Auftrag eingestellt werden sollen. Wurde ein anderes Unterverzeichnis ausgewählt, wird dieses beim nächsten Auftrag wiederum angeboten. Klicken Sie die gewünschte Datei an und drücken Sie dann auf die Schaltfläche [***Öffnen***].



Im Anschluss wird die zu übertragende Datei zur Kontrolle in einem Fenster angezeigt. Diese Anzeige ist ebenfalls abhängig vom durch die Auftragsart festgelegten Dateiformat. Der vollständige Pfad wird im Feld "**Datei**" angezeigt.

Tritt bei der Auswahl ein Fehler auf, wird die betreffende Datei in einem gesonderten Fenster mit einem kurzen Fehlerhinweis angezeigt.

Über die normalen Anzeigefunktionen des Fensters haben Sie u. a. die Möglichkeit, die Informationen für Ihre Unterlagen auszudrucken. Dies ist beispielsweise bei Zahlungsaufträgen sinnvoll.

Bei Abholaufträgen wird die im weiteren Programmverlauf abgeholte Datei im Verzeichnis ..\MCCWIN unter dem in der Detailanzeige des DFÜ-Auftrages angezeigten Dateinamen gespeichert. Der Dateiname setzt sich aus einem konstanten Teil "BWM", einem die Datei

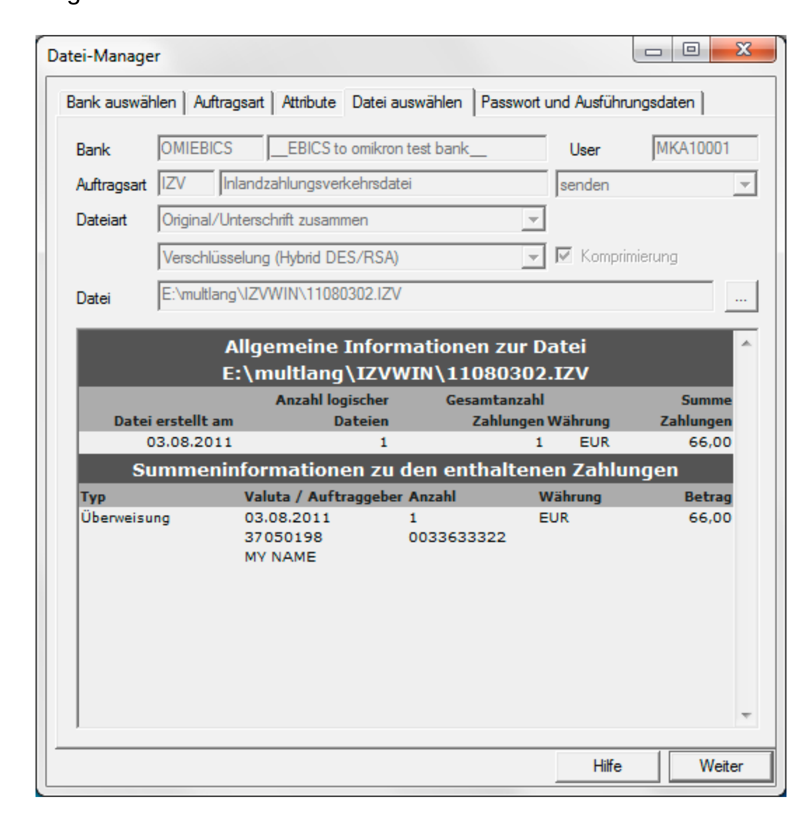


charakterisierenden Kennzeichen, der vom Programm vergebenen 4-stelligen Auftragsnummer sowie der Auftragsart als Extension zusammen.

Beispiel:

BWMDA0A5.STA

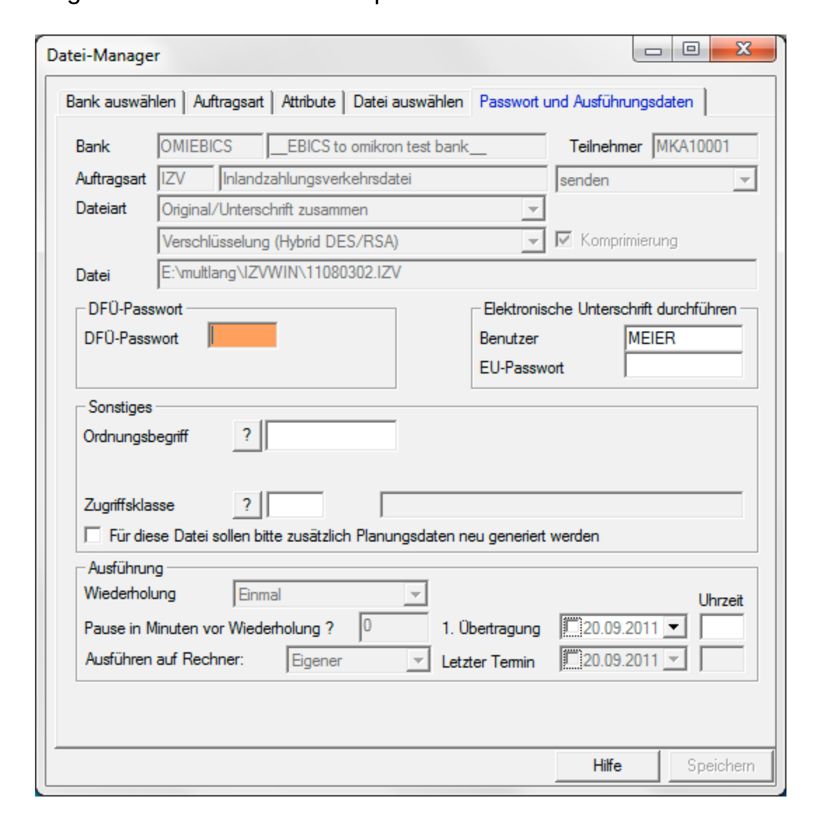
BWM : konstanter Teil
D : Dateikennzeichen
A0A5 : Auftragsnummer
STA : Auftragsart





Registerkarte "Passwort und Ausführungsdaten"

Als letzter Schritt bei Erstellung eines DFÜ-Auftrages ist die **Eingabe des DFÜ-Passwortes** vorzunehmen (ggf. eine EU). Das von der jeweiligen Bank abhängige DFÜ-Passwort ist zur Durchführung der Aufträge zwingend erforderlich. Sie benötigen für alle zur Durchführung von DFÜ-Aufträgen vorgesehenen Banken ein separates DFÜ-Passwort.



DFÜ-Passwort:

DFÜ-Passwort

Das DFÜ-Passwort kann bei Aufträgen, die aus Modulen heraus eingestellt wurden, nicht verändert werden. Bei DFÜ-Aufträgen, die einen Abholvorgang betreffen, ist eine Änderung des Passwortes an dieser Stelle möglich.

Das Logon am Bank-Server erfolgt bei EBICS nicht mehr mit einen DFÜ-Passwort, sondern mit einer Signatur. Für den Zugriff auf den hierfür benötigten privaten Schlüssel wird gleichwohl ein Passwort benötigt. Hierfür wird das an allen notwendigen Stellen im Programm vorhandene Eingabe-Feld "DFÜ-Passwort" herangezogen.

Elektronische Unterschrift durchführen:

Benutzername und Passwort für die Elektronische Unterschrift

Wurde bei Sendeaufträgen auf der *Registerkarte Attribute* ein Verfahren mit Elektronischer Unterschrift gewählt, kann anschließend der **Benutzer**, der die EU leistet (vorbelegt mit dem aktuell angemeldetem Benutzer) und das **EU-Passwort** eingegeben werden.

Sonstiges:

Ordnungsbegriff

Analog zum früheren DAD-Namen kann ein Ordnungsbegriff vergeben werden. Danach kann selektiert werden und damit die Abarbeitung strukturiert werden.



Zugriffsklasse

Im Datei-Manager kann die Zugriffsklasse bei der Neuaufnahme einer Datei ebenfalls gesetzt werden (vgl. Kapitel 7.8).

Für diese Datei sollen zusätzlich Planungsdaten neu generiert werden

Um z. B. für Dateien aus Fremdsystemen, die über den Datei-Manager versandt werden, ebenfalls Planungsdaten zu generieren, müssen Sie dieses Kontrollkästchen markieren. Bei Vorhandensein der entsprechenden Konten werden dann die Daten (ggf. mit mit eigenem Ordnungsbegriff und einer Zugriffsklasse) in die Planungsdaten eingestellt.
Die Markierung dieses Kontrollkästchens kann über den Parameter **Planungsdaten generieren im Dateimanager** für jede Auftragsart vorbelegt werden (s. Basis-Kapitel 6.4.1: *Registerkarte Auftragsarten*).

<u>Ausführung:</u>

Wiederholung

Sobald Sie die Listbox über den nach unten weisenden Pfeil öffnen, können Sie bei Abholaufträgen den Wiederholungsrhythmus für den DFÜ-Auftrag festlegen. Bei Sendeaufträgen ist eine Änderung des Wiederholungsrhythmus nicht möglich (ebenso: Letzter Termin).

Zur Auswahl stehen:

- Einmal
- Jede Stunde
- Alle 3 Stunden
- Alle 6 Stunden
- Zweimal täglich
- Einmal täglich
- Jeden Wochentag
- Dreimal pro Woche
- Einmal pro Woche
- Zweimal pro Monat
- Einmal pro Monat
- Jedesmal (tägl. bis erfolgreich)

Der Rhythmus "Jedesmal (tägl. bis erfolgreich)" startet (abhängig von der unten eingetragenen Wartezeit) einen Auftrag immer wieder, <u>bis</u> dieser <u>einmal am</u> aktuellen <u>Tag</u> mit Antwortcode 1 <u>erfolgreich</u> beendet wird. Dieser Rhythmus sollte für Abholaufträge gewählt werden, die typischerweise einmal am Tag erfolgreich sein sollten (z. B. Kontoauszüge abrufen).

Der Rhythmus "Einmal" eignet sich für Aufträge, die bei Bedarf manuell angestoßen werden sollen (z. B. Abruf der EU-Protokolle). Für diesen Anwendungsfall sollte zusätzlich das Kontrollkästchen "Abholen immer manuell anstoßen über Icon" aktiviert werden (s. Kapitel 5.1.2.2: *Registerkarte Nachverarbeitung und Übertragungsparameter*).
Wie sie Abholaufträge komfortabel mit Hilfe eines Assistenten anlegen können, erfahren Sie in Kapitel 5.2: *Assistent für das Abholen von Daten bei mehreren Banken / Rundruf* .

Pause in Minuten vor Wiederholung

Geben Sie hier eine Zahl ein, wenn vor der Wiederholung eine gewisse Zeit (in Minuten) gewartet werden soll.
Bei Auswahl des Ausführungsrhythmus "Jedesmal (tägl. bis erfolgreich)" wird das Feld mit dem Wert 30 (Minuten) vorbelegt.

1. Übertragung

In dieses Feld können Sie Datum und Uhrzeit für die erstmalige Ausführung eines DFÜ-Auftrages eintragen. Soll die Erstübertragung eines DFÜ-Auftrages nicht zu einem bestimmten Zeitpunkt erfolgen, so lassen Sie das Feld leer.



Letzter Termin

Wollen Sie den Ausführungszeitraum des DFÜ-Auftrages begrenzen, tragen Sie hier das Datum und die Uhrzeit für die letztmalige Auftragsausführung ein. Das Feld kann "leer" bleiben, wenn der Auftrag in einem bestimmten Rhythmus ohne Auslaufdatum übertragen werden soll oder nur eine einmalige Übertragung stattfindet. Eine Editierung ist nur dann möglich, wenn der Auftrag nicht über ein Modul in in den Datei-Manager eingestellt wurde.

Sind in den Feldern für "1. Übertragung" und "Letzter Termin" Uhrzeiten vorgegeben, so können Abholaufträge jeweils nur innerhalb des für sie definierten Zeitfensters ausgeführt werden, z. B. stündlich von 0.00 bis 24.00 Uhr (ausschließlich! D. h., um 24.00 Uhr wird kein Auftrag mehr ausgeführt).

Ausführen auf Rechner:

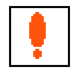
Nach einer Installation des Programms auf Ihrem lokalen Rechner (Standardinstallation) wird dieses Feld immer mit "Eigener" belegt, d. h. sämtliche DFÜ-Aufträge werden auf Ihrem lokalen PC ausgeführt.

Handelt es sich allerdings um eine Netzwerkinstallation oder Einzelplatzinstallation auf einem Netzwerklaufwerk, so kann mit Hilfe dieser Auswahlliste festgelegt werden, von welchem zur Durchführung der Datenfernübertragung geeigneten Rechner die Ausführung des Kommunikationsauftrages erfolgen soll.

Für die Auswahl des DFÜ-Rechners werden nur die Rechner in der Liste angeboten, für die DFÜ-Parameter definiert sind. Ein einmal ausgewählter Rechner wird bei jeder folgenden DFÜ als Standard vorgeschlagen.

Zeitraum (in dem Daten abgeholt werden sollen)

Die Felder "Daten von" und "Daten bis" beziehen sich nur auf Abholaufträge. Bei der Neuaufnahme eines DFÜ-Auftrages können Sie hier angeben, über welchen Zeitraum sich die bei der Bank abzuholenden Daten (z. B. Kontoinformationen) erstrecken sollen. Lassen Sie das Feld "Daten von/bis" unmarkiert, werden alle auf dem Bankrechner zur Verfügung gestellten und noch nicht abgeholten Daten zu der angegebenen Dateiart abgeholt.



Nur wenn Sie das Feld "Daten von/bis" unmarkiert lassen und keine Datumsbegrenzung eintragen, können Sie sicher sein, dass Sie auch alle auf der Bankseite für Sie bereitgestellten Daten erhalten.

Nach Drücken der Schaltfläche [***Speichern***] erfolgt die Leistung der Elektronischen Unterschrift.
Bei Abholaufträgen wird die Aufnahme des neuen Auftrags direkt durch Betätigen der Schaltfläche [***Speichern***] abgeschlossen.



5.1.2 Detailansicht Datei-Manager

Um eine Detailansicht eines einzelnen Datensatzes zu erhalten, wählen Sie zunächst den entsprechenden Datenbankeintrag durch Cursorpositionierung und bestätigendes <**Return**> oder einen Doppelklick aus. Sie können eine Datensatz auch durch Anklicken mit der rechten Maustaste und anschließender Auswahl des Menüpunktes -**Detailanzeige**- öffnen.

Es öffnet sich eine Dialogbox mit verschiedenen Registerkarten. Da es sich bei der Detailansich im Wesentlichen um eine **Anzeigefunktion** handelt, können hier mit einer Ausnahme die Daten nur angesehen, aber nicht mehr bearbeitet werden. Die entsprechenden Felder erscheinen daher inaktiv.

Der Kopfbereich jeder einzelnen Registerkarte enthält den **Dateiname**n der aufgerufenen Datei (inklusive vollständiger Pfadangabe) sowie allgemeine Informationen zur Datei angegeben, wie **BPD-Name**, Status, **Dateiart**, **Attribut**, **Auftragsnummer** und bei Ablehnung des Auftrags Name des Benutzer, der den Auftrag abgelehnt hat sowie Datum und Uhrzeit der Ablehnung.

Zugriffsklasse

In der Detailanzeige kann die Zugriffsklasse ebenfalls gesetzt werden, soweit sie nicht automatisch aus einem Zahlungsverkehrsmodul übergeben wurde.

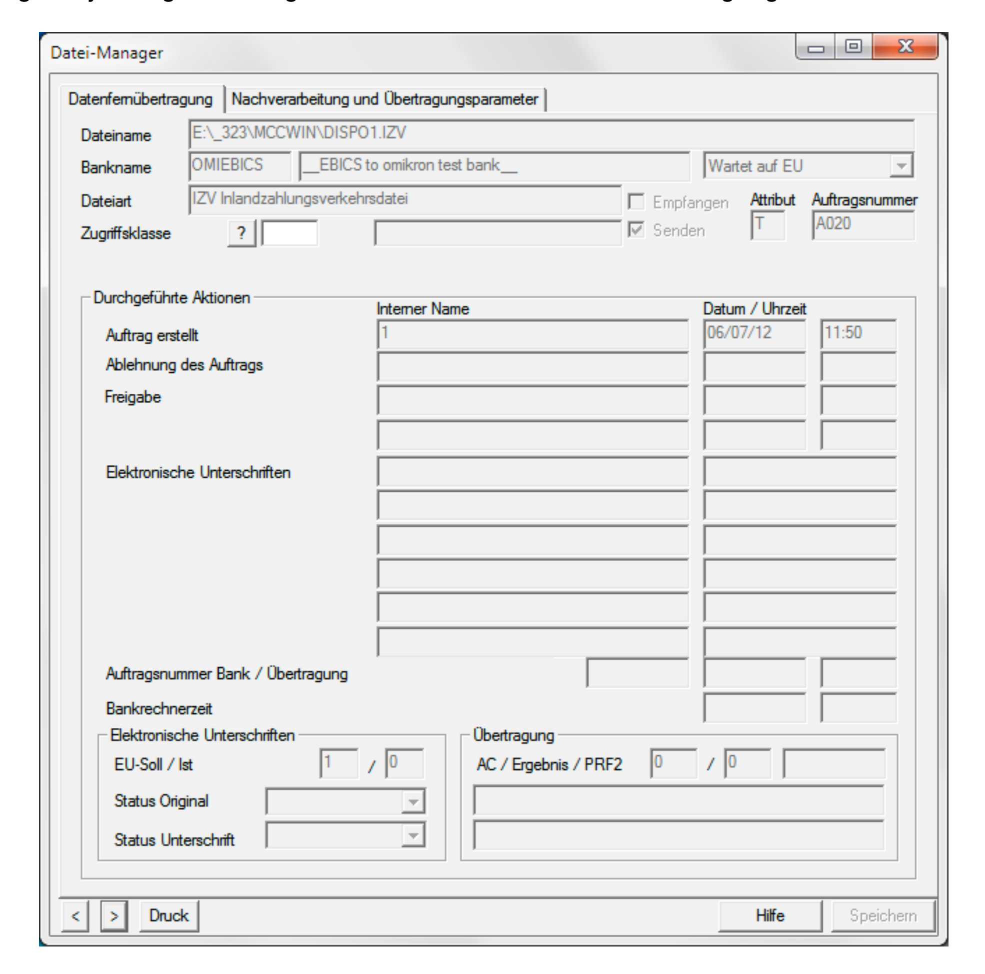
Der Bereich der Registerkarten darunter unterscheidet sich.

5.1.2.1 *Registerkarte Datenfernübertragung*
5.1.2.2 *Registerkarte Nachverarbeitung und Übertragungsparameter*
5.1.2.3 *Registerkarte DFÜ-Protokoll / EU-Protokoll*



5.1.2.1 Registerkarte Datenfernübertragung

Die Felder der *Registerkarte Datenfernübertragung* geben Informationen über den Verlauf der Bearbeitung des jeweiligen Auftrages und zum Stand der Datenübertragung.



Durchgeführte Aktionen:

Sie erfahren jeweils mit Angabe des Benutzers (Interner Name), Datum und Uhrzeit der Aktion, wer den Auftrag erstellt hat, wer den Auftrag abgelehnt hat, wer den Auftrag freigeben hat (bis zu zwei Freigaben), wer Unterschriften geleistet hat (bis zu sechs Elektronische Unterschriften) und wann die Datei übertragen wurde.
Nach der Umschaltung auf die neue Protokollversion H004 gemäß EBICS-Spezifikation Version 2.5 werden die Auftragsnummern für Sendeaufträge vom Banksystem vergeben, nicht mehr vom Kundensystem. Dies ist jedoch nur für die Abstimmung von Bank- und Kundensystem von Belang (z. B. für Protokolle oder verteilte Unterschrift). Daher bleibt die Verarbeitung unverändert, die von Banksystem vergebene Auftragsnummer wird aber für Analysezwecke hier als **Auftragsnummer Bank** angezeigt.
Außerdem finden Sie hier Datum und Uhrzeit der **Übertragung** auf Kundenseite und auf Bankrechnerseite (Bankrechnerzeit).

Elektronische Unterschriften:

Hier sind alle Informationen, die die Elektronische Unterschrift betreffen, zusammengefasst. So finden Sie hier die Soll- und die Ist-Anzahl der Elektronischen Unterschriften sowie den Status von Originaldatei und Unterschriftsdatei.



Übertragung:

Das erste Feld nimmt den Antwort-Code (= **AC**) auf, der von der Bank als Rückgabewert bei fehlerfreier Ausführung des DFÜ-Auftrages sowie bei fehlerhafter und abgebrochener Übertragung zurückgegeben wird. Die Zahl "1" bedeutet eine fehlerfreie Durchführung des jeweiligen DFÜ-Auftrages. Die Bedeutung der weiteren Antwortcodes finden Sie in Kapitel 5.4: *Antwort-Codes*.

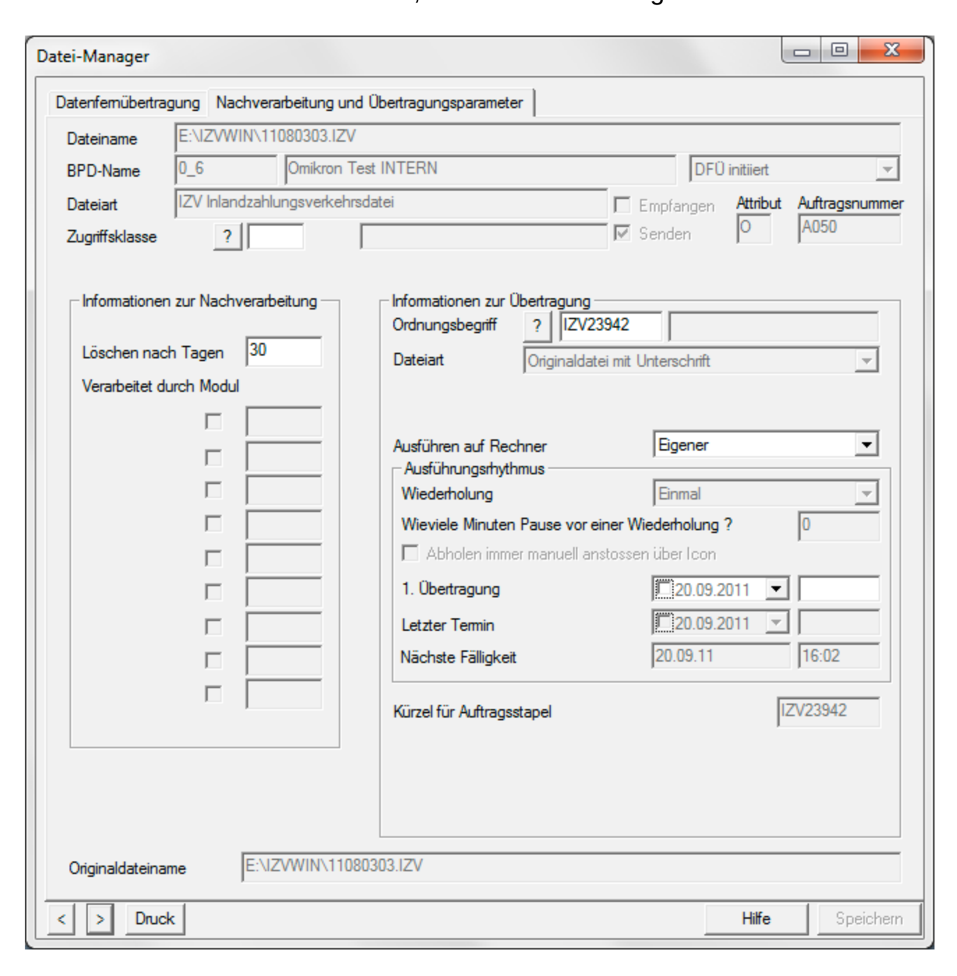
Dahinter folgt das **Ergebnis** (Sub-Antwortcode) und eine Prüfsumme (**PRF2**).
Schließlich zwei Zeilen mit dem Ergebnistext sowie dem Namen der zugehörigen Originaldatei.

5.1.2.2 Registerkarte Nachverarbeitung und Übertragungsparameter

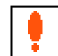
Informationen zur Nachverarbeitung:

Die Registerkarte *Nachverarbeitung und Übertragungsparameter* enthält u. a. eine Möglichkeit zur weiteren Behandlung der Datei nach der DFÜ.
Editiert werden kann hier nämlich das Feld "**Löschen nach Tagen**". Für die Zeit der dort eingetragenen Anzahl von Tagen bleibt die Datei im System gespeichert, auch wenn keine Applikation "starkes Interesse" an diesem Dateityp angemeldet hat. Nach Ablauf dieser Aufbewahrungsfrist wird die Datei (und der Eintrag in der Datenbank) ohne weitere Rückfrage gelöscht.

Bitte beachten Sie:
Nur wenn für die jeweilige **Auftragsart** das Kontrollkästchen **Datei nach Verarbeitung durch alle Module löschen** gesetzt ist, wird eine empfangene Datei, nachdem alle Module mit Interesse diese Datei verarbeitet haben, beim nächsten Programmstart im Automaten gelöscht.



Darunter werden die Applikationen angezeigt, die "Interesse" an der Datei angemeldet haben ("**Verarbeitet durch Modul**"). Falls die Verarbeitung durch ein Modul stattgefunden hat, wird dies duch Angabe der Uhrzeit hier angegeben.



Durch die Vergabe von "Interessen" wird sichergestellt, dass alle Applikationen, die Zugriff auf bestimmte Auftragsarten haben müssen, diese auch zur Verarbeitung genau einmal zur Verfügung gestellt bekommen.



Das Cashmanagement hat z. B. ein "**starkes Interesse**" an den mit der Auftragsart "STA" von der Bank abgeholten Kontoinformationen. Das bedeutet, dass die Daten - unabhängig von der festgelegten Verwahrdauer - solange nicht gelöscht werden, bis die mit "starkem Interesse" angemeldete(n) Applikation(en) die so gekennzeichneten Daten verarbeitet hat (haben).

Meldet eine Applikation "**normales Interesse**" an, werden die zur Verarbeitung erforderlichen Daten gelöscht, wenn die Verwahrdauer überschritten wird. Der Löschvorgang erfolgt unabhängig davon, ob die Applikation die Daten bereits verarbeitet hat oder nicht.

Informationen zur Übertragung:

Analog zum früheren DAD-Namen wird ein **Ordnungsbegriff** geführt. Danach kann selektiert werden und damit die Abarbeitung strukturiert werden.

Dateiart

Die Art der zu übertragenden bzw. abzuholenden Datei wird angezeigt. Es wird unterschieden zwischen

- Originaldatei ohne Unterschrift
- Originaldatei mit Unterschrift
- Unterschriftsdatei.

Abhängig vom eingesetzten DFÜ-Verfahren sind hier weitere Attribute wählbar wie z. B. die **Verschlüsselung** über eine Auswahlliste bei den Verfahren FTAM bzw. FTP oder eine **Komprimierung** mittels FLAM über ein entsprechendes Kontrollkästchen.

Ausführen auf Rechner

Nach einer Installation des Programms auf Ihrem lokalen Rechner (Standardinstallation) wird dieses Feld immer mit "Eigener" belegt, d. h. sämtliche DFÜ-Aufträge werden auf Ihrem lokalen PC ausgeführt.

Handelt es sich allerdings um eine Netzwerkinstallation oder Einzelplatzinstallation auf einem Netzwerklaufwerk, so kann mit Hilfe dieser Auswahlliste festgelegt werden, von welchem zur Durchführung der Datenfernübertragung geeigneten Rechner die Ausführung des Kommunikationsauftrages erfolgen soll.

Ausführungsrhythmus:

Der **Ausführungsrhythmus** für wiederkehrende Aufträge wird hier ebenfalls hinterlegt. Als Ausführungsrhythmus stehen im Feld "**Wiederholung**" zur Auswahl:

- Einmal
- Jede Stunde
- Alle 3 Stunden
- Alle 6 Stunden
- Zweimal täglich
- Einmal täglich
- Jeden Wochentag
- Dreimal pro Woche
- Einmal pro Woche
- Zweimal pro Monat
- Einmal pro Monat
- Jedesmal (tägl. bis erfolgreich)

Durch Anwahl des entsprechenden Eintrages in der Auswahlliste übernehmen Sie den gewünschten Ausführungsrhythmus.



Der Rhythmus "Jedesmal (tägl. bis erfolgreich)" startet (abhängig von der unten eingetragenen Wartezeit) einen Auftrag immer wieder, bis dieser einmal am aktuellen Tag mit Antwortcode 1 erfolgreich beendet wird. Dieser Rhythmus sollte für Abholaufträge gewählt werden, die typischerweise einmal am Tag erfolgreich sein sollten /z. B. Kontoauszüge abrufen).

Der Rhythmus "Einmal" eignet sich für Aufträge, die bei Bedarf manuell angestoßen werden sollen (z. B. Abruf der EU-Protokolle). Für diesen Anwendungsfall sollte zusätzlich das Kontrollkästchen "**Abholen immer manuell anstoßen über Icon**" aktiviert werden (s. unten).

Pause in Minuten vor Wiederholung

Geben Sie hier eine Zahl ein, wenn vor der Wiederholung eine gewisse Zeit (in Minuten) gewartet werden soll.
Bei Auswahl des Ausführungsrhythmus "Jedesmal (tägl. bis erfolgreich)" wird das Feld mit dem Wert 30 (Minuten) vorbelegt.

Abholen immer manuell anstoßen über Icon

Soll ein Abholauftrag immer manuell über das Icon gestartet werden, so ist dieses Kontrollkästchen zu aktivieren.
Wenn Sie beim Definieren der Abholaufträge über den Assistenten festgelegt haben, dass Sie die Kommunikation manuell starten möchten (siehe Kapitel 5.2: *Assistent für das Abholen von Daten bei mehreren Banken / Rundruf*), ist das Kontrollkästchen bereits markiert.

1. Übertragung
Letzter Termin

Das Datum für die erstmaligen Übertragung einer Datei hinterlegen Sie in dem entsprechenden Eingabefeld mit Datum (einstellbar über den Kalender) und Uhrzeit. Bei Übertragungen mit Elektronischer Unterschrift gilt das Datum jeweils für Originaldatei und Unterschriftsdatei.
Soll der Kommunikationsauftrag nur bis zu einem bestimmten Termin in dem zuvor angegebenen Ausführungsrhythmus ausgeführt werden, so legen Sie auch einen letztmaligen Ausführungstermin mit Datum (einstellbar über den Kalender) und Uhrzeit fest. Der Kommunikationsauftrag wird nicht mehr ausgeführt, wenn der letzte Termin überschritten wurde.

Nächste Fälligkeit

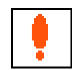
Das Feld "Nächste Fälligkeit" gibt an, wann ein Kommunikationsauftrag zum nächsten Mal zur Ausführung ansteht. Auf der Basis des vorgegebenen Rhythmus wird der nächste Ausführungszeitpunkt (Datum und Uhrzeit) ermittelt und angezeigt.
Zur Anzeige des nächsten Fälligkeitszeitpunktes in der Übersicht des Dateimanagers s. Kapitel 5.1.1: *Datenbankübersicht Datei-Manager*.

Kürzel für Auftragsstapel

Um Kommunikationsaufträge in Gruppen zusammenfassen zu können, können Sie mit einem gemeinsamen Kürzel belegt werden. Das Kürzel (max. 8 Stellen alphanumerisch) wird beim Anlegen sogenannter Auftragsstapel vergeben (s. Kapitel 5.2: *Assistent für das Abholen von Daten bei mehreren Banken / Rundruf*).
Ist ein Auftrag einem solchen Auftragsstapel zugeordnet, so wird dessen Kürzel hier angezeigt.

Zeitraum (in dem Daten abgeholt werden sollen)

Die Felder "Daten von" und "Daten bis" beziehen sich nur auf Abholaufträge. Beim Abholen historischer Daten können Sie hier angeben, über welchen Zeitraum sich die bei der Bank abzuholenden Daten (z. B. Kontoinformationen) erstrecken sollen. Lassen Sie das Feld "Daten von/bis" unmarkiert, werden alle auf dem Bankrechner zur Verfügung gestellten und noch nicht abgeholten Daten zu der angegebenen Dateiart abgeholt.



Nur wenn Sie das Feld "Daten von/bis" unmarkiert lassen und keine Datumsbegrenzung eintragen, können Sie sicher sein, dass Sie auch alle auf der Bankseite für Sie bereitgestellten Daten erhalten.



 **Bitte beachten Sie:**

Bei manuell auszuführenden Abholaufträgen sind die letztgenannten Felder generell deaktiviert und reine Anzeigefelder. Die Pflege dieser Felder ist nur über den Assistenten zum Abholen von Daten bei mehreren Banken möglich (s. Kapitel 5.2).



5.1.2.3 Registerkarte DFÜ-Protokoll / EU-Protokoll

Auf der *Registerkarte DFÜ-/EU-Protokoll* werden die Ergebnisse der abgeholten Bankprotokolle (z. B. zur Unterschriftsprüfung) angezeigt. Diese Registerkarte schiebt sich, sofern vorhanden, zwischen die beiden übrigen Registerkarten (die Sprache der Inhalte ist abhängig vom jeweiligen Bankrechner).
Mit EBICS 2.5 kann alternativ zur bekannten Auftragsart PTK mit der Auftragsart HAC ein Kundenprotokoll im XML-Format abgerufen werden. Dies wird ebenfalls dem zugehörigen Dateimanagereintrag zugeordnet und zur Anzeige analog PTK aufbereitet.

Beispiel:

Datei-Manager

Datenfernübertragung | DFÜ/EU-Protokoll | Nachverarbeitung und Übertragungsparameter

Dateiname: I:\MC323R2\MCCWIN\SAV\12070602.IZV

Bankname: EBC323KK | UFA-EBICSSERVER 3.22 auf LW K. | EU-Prüfung OK

Dateiart: IZV Inlandzahlungsverkehrsdatei | Empfangen | Attribut: B | Auftragsnummer: A0OB

Zugriffsklasse: ? | Senden

```
06.07.12 10:39:30     FILE_UPLOAD 120706105032529
         Hostname   : EBICSUFA
         Order      : IZV B03R
         Customer   : EBC323KK Ebics BR 323
         User       : EBC323TT
         Result     : TS01 Die Übertragung der Datei war erfolgreich

06.07.12 10:39:30     ES_VERIFICATION 120706105032529
         Hostname   : EBICSUFA
         Order      : IZV B03R
         Customer   : EBC323KK Ebics BR 323
         User       : EBC323TT
         User       : EBC323T2
         Result     : DS01 Elektronische Unterschrift(en) korrekt

06.07.12 10:39:30     ORDER_HAC_FINAL_POS 120706105032529
         Hostname   : EBICSUFA
         Order      : IZV B03R
         Customer   : EBC323KK Ebics BR 323
         User       : EBC323TT

         ============================================================
          G U T S C H R I F T E N
          Bankleitzahl              : 20090700
          Kontonummer               : 0030004712
          Auftraggeber              : AUFTRAGGEBER 1
          Erstellungsdatum          : 04.07.12
          Anzahl der Zahlungssätze  : 1
          Summe der Beträge (EUR)   : 67,00
          Summe der Kontonummern    : 30.004.712
          Summe der Bankleitzahlen  : 20.090.700
          Ausführungstermin         : 04.07.2012
         ----------------------------------------------------
         ============================================================
```

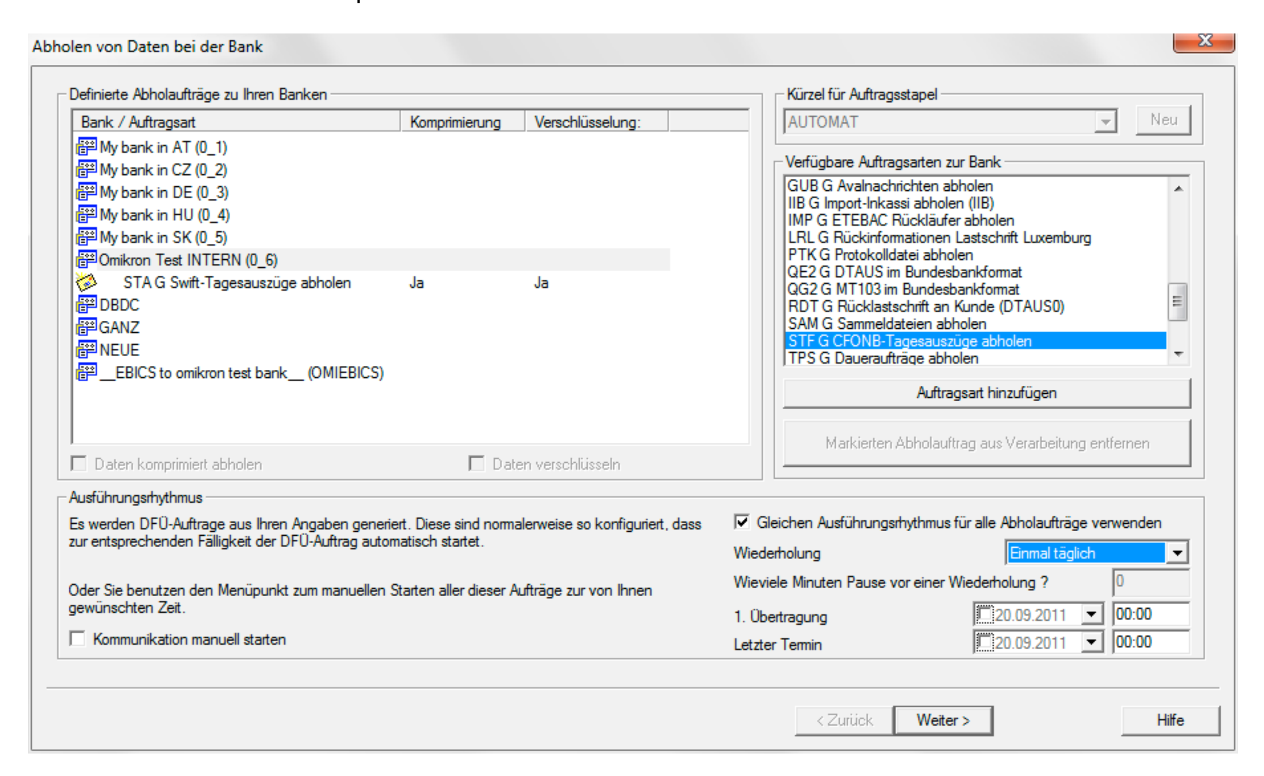
< | > | Druck | Hilfe | Speichern



5.2 Assistent für das Abholen von Daten bei mehreren Banken / Rundruf

DFÜ-Prozesse werden sinnvollerweise im Hintergrund ausgeführt, damit der Anwender - auch wenn die DFÜ läuft - mit anderen Funktionen des Programms arbeiten kann. Ein typisches Beispiel für einen solchen Prozess ist das Abholen von Kontoinformationen. Sie können vollautomatisch zu definierten Zeiten alle gewünschten Informationen, wie Kontoauszüge, Devisenkurse, Vormerkposten, FTAM-Protokolle o. ä. von allen Ihren Banken abholen (sogenannte **Rundruf-Funktion**).
Sie können die Abholaufträge aber auch jederzeit per Mausklick über ein Icon der Symbolleiste manuell starten.

Um die Art der auszuführenden Abholaufträge festzulegen bzw. zu ändern, wählen Sie unter -Kommunikation- den Menüpunkt -Assistent Abholen von Daten bei mehreren Banken-.



Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um die Abholaufträge bei den verschiedenen Banken zu definieren.

Indem Sie über die Funktion "Auftragsstapel" unterschiedliche Bezeichnungen vergeben, können verschiedene "Stapel" von Abholaufträgen verwaltet werden (ähnlich wie in älteren Versionen mittels DAD). Durch wiederholtes Aufrufen des Assistenten über den Menüpunkt können so verschiedene Auftragsstapel für unterschiedliche Zwecke erstellt werden.

Sollen Abholaufträge als "Stapel" zusammengefasst werden, so können Sie eine Bezeichnung für einen solchen "**Auftragsstapel**" über das Listenfeld "Kürzel für Auftragsstapel" auswählen (der Auftragsstapel mit dem Kürzel "Automat" mit dem gleichlautenden Ordnungsbegriff [im Dateimanager] steht als Standard-Eintrag immer zur Verfügung und ihm können sofort Abholaufträge individuell zugeordnet werden).
Neue Bezeichnungen für Auftragsstapel erzeugen Sie über die danebenliegende Schaltfläche [***Neu***].
Nach Drücken der Schaltfläche werden Sie aufgefordert, ein Kürzel (max. 8 Stellen alphanumerisch) für den neuen Auftragsstapel einzugeben. Bestätigen Sie abschließend Ihre Eingabe mit [***OK***].





1 **Auswahl der Banken bzw. Auftragsarten/Definition der Abholaufträge**

Wählen Sie aus der Liste der Banken () mittels Mausklick jeweils eine Bank aus, von der Sie Daten abholen möchten.

Markieren Sie anschließend eine der **verfügbare**n Abhol-**Auftragsarten zu** de**r** markierten **Bank**. Durch Drücken der Schaltfläche [***Auftragsart hinzufügen***] fügen Sie die gewählte Auftragsart der Liste der **definierte**n **Abholaufträge zu Ihren Banken** hinzu.
Die von Ihnen definierten Aufträge werden in der Liste jeweils unterhalb der Bank aufgeführt ().

Zusätzlich können Sie, wenn Sie den Abholauftrag in der Liste per Mausklick markieren und es vom Übertragungsverfahren her vorgesehen ist, entscheiden, ob Sie die "**Daten komprimiert abholen**" und/oder ob Sie die "**Daten verschlüssel**t übertrage**n**" möchten.

Wiederholen Sie den Vorgang jeweils für weitere Banken, von denen Sie Daten abholen möchten.

Zum Entfernen von Abholaufträgen markieren Sie bitte den betreffenden Abholauftrag in der Liste und betätigen anschließend die Schaltfläche [***Markierten Abholauftrag aus Verarbeitung entfernen***].

Ausführungsrhythmus:

Für die Rundruf-Funktion werden aus den hier gemachten Angaben sogenannte DFÜ-Aufträge generiert, die zu(m) vordefinierten Zeitpunkt(en) die Datenübertragung automatisch starten.

Sie können fällige Aufträge aber auch selber zu einer beliebigen von Ihnen gewünschten Zeit über das entsprechende Icon starten (s. u.), wenn Sie das Kontrollkästchen "**Kommunikation manuell starten**" markieren.
Die Editierung von Wiederholungsrhythmen (zu den Einstellungen s. u.) ist auch bei diesen manuell zu startenden Abholaufträgen möglich. Damit können -ähnlich wie früher in einer DAD- innerhalb eines Stapels Abholaufträge mit unterschiedlichen Ausführungsrhythmen und -zeiträumen hinterlegt werden, die **nur bei Fälligkeit** ausgeführt werden, sobald der Stapel über das Icon angestoßen wird.

☞ **Bitte beachten Sie:**

Vorgaben in diesem Bereich schränken die Ausführbarkeit manuell zu startender Abholaufträge ein (da sie bei Nichterfüllung hier gewählter Kriterien als "nicht fällig" gelten).

So kann z. B. ein Abholauftrag mit dem Wiederholrhythmus "Jede Stunde" nach dem ersten manuellen Ausführen (des Stapels) frühestens nach einer Stunde durch manuelles Starten erneut ausgeführt werden. Erst dann ist er wieder fällig. Wird der Stapel in der Zwischenzeit manuell gestartet, bleibt der betreffende Abholauftrag bei der Ausführung unberücksichtigt.

Sind in den Feldern für "1. Übertragung" und "Letzter Termin" Uhrzeiten vorgegeben, so können die Abholaufträge jeweils nur innerhalb des für sie definierten Zeitfensters durch manuelles Starten des entsprechenden Auftragsstapels ausgeführt werden, z. B. täglich



in der Zeit von 9.00 bis 17.00 Uhr (ausschließlich! D. h., um 17.00 Uhr wird kein Auftrag mehr ausgeführt).

Über diese Einstellung (nur Uhrzeit, kein Datum) lässt sich auch die Ausführung automatischer Aufträge, die mehrfach am Tag wiederholt werden sollen, auf ein bestimmtes Zeitfenster beschränken.

Der Rundruf erfolgt bei allen Banken zur selben Zeit, wenn Sie das Kontrollkästchen "**Gleichen Ausführungsrhythmus für alle Abholaufträge verwenden**" markieren. Möchten Sie Rundrufe bei den verschiedenen Banken zu unterschiedlichen Zeiten starten oder mehrere Rundrufe täglich definieren, müssen Sie die Markierung entfernen und für jeden Abholauftrag separat einen Ausführungsrhythmus erfassen.

Wiederholung

Sobald Sie die Listbox über den nach unten weisenden Pfeil öffnen, können Sie bei Abholaufträgen den Wiederholungsrhythmus für den DFÜ-Auftrag festlegen.

Zur Auswahl stehen:

- Einmal
- Jede Stunde
- Alle 3 Stunden
- Alle 6 Stunden
- Zweimal täglich
- Einmal täglich
- Jeden Wochentag
- Dreimal pro Woche
- Einmal pro Woche
- Zweimal pro Monat
- Einmal pro Monat
- Jedesmal (tägl. bis erfolgreich)

Der Rhythmus "Einmal" eignet sich für Aufträge, die bei Bedarf manuell angestoßen werden sollen (z. B. Abruf der EU-Protokolle). Für diesen Anwendungsfall sollte zusätzlich das oben genannte Kontrollkästchen "Kommunikation manuell starten" aktiviert werden.

Der Rhythmus "Jedesmal (tägl. bis erfolgreich)" startet (abhängig von der unten eingetragenen Wartezeit) einen Auftrag immer wieder, bis dieser einmal am aktuellen Tag mit Antwortcode 1 erfolgreich beendet wird. Dieser Rhythmus sollte für Abholaufträge gewählt werden, die typischerweise einmal am Tag erfolgreich sein sollten (z. B. Kontoauszüge abrufen).
Auch bei einer Ausführung aus dem Dateimanager heraus wird der folgende Wartezyklus beachtet.

Pause in Minuten vor Wiederholung

Geben Sie hier eine Zahl ein, wenn vor der Wiederholung eine gewisse Zeit (in Minuten) gewartet werden soll.
Bei Auswahl des Ausführungsrhythmus "Jedesmal (tägl. bis erfolgreich)" wird das Feld mit dem Wert 30 (Minuten) vorbelegt.
Die Eingabe von "0" entspricht ebenfalls diesem Wert (Default). Um zu häufige Abholvorgänge zu verhindern, wird bei einem Rhythmus "Jedesmal (tägl. bis erfolgreich)" und einer Pause < 10 Minuten die Zeitspanne bis zur nächsten Übertragung automatisch auf "10" Minuten hochgesetzt.

1. Übertragung

In diesen Feldern können Sie Datum und/oder Uhrzeit für die erstmalige Ausführung eines DFÜ-Auftrages eintragen. Soll die Erstübertragung eines DFÜ-Auftrages nicht zu einem bestimmten Datum/Zeitpunkt erfolgen, so lassen Sie die entsprechenden Felder leer.



Letzter Termin

Wollen Sie den Ausführungszeitraum des DFÜ-Auftrages begrenzen, tragen Sie hier das Datum und/oder die Uhrzeit für die letztmalige Auftragsausführung ein. Die entsprechenden Felder können "leer" bleiben, wenn der Auftrag in einem bestimmten Rhythmus ohne Auslaufdatum/-uhrzeit übertragen werden soll oder nur eine einmalige Übertragung stattfindet.

Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].

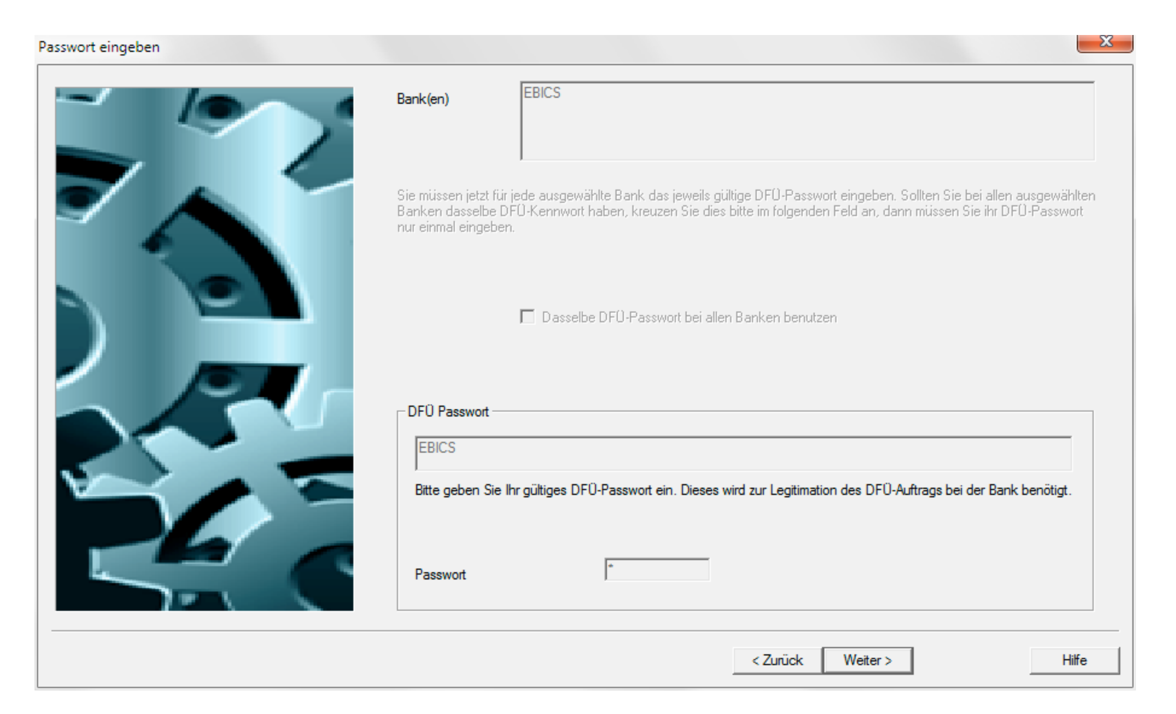
2 **DFÜ-Passwort eingeben**

Geben Sie anschließend jeweils Ihr gültiges DFÜ-Passwort ein. Es wird zur Legitimation des DFÜ-Auftrages bei der Bank benötigt.
Die Passwortvergabe erfolgt verdeckt, d. h. jeder Tastendruck wird durch ein * (Sternchen) dargestellt.

Verwenden Sie bei allen ausgewählten Banken dasselbe DFÜ-Passwort, markieren Sie bitte das entsprechende Kontrollkästchen "**Dasselbe DFÜ-Passwort bei allen Banken benutzen**". Die Passwort-Abfrage erfolgt dann nur einmal.

Ihre Eingabe wird gespeichert. Beim nächsten Aufruf Ihrer Bank entfällt daher Schritt 2. Erst wenn Sie z. B. weitere Auftragsarten hinzufügen, werden Sie zur Legitimation wieder nach dem DFÜ-Passwort gefragt.

Sie schließen die Passworteingabe ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.

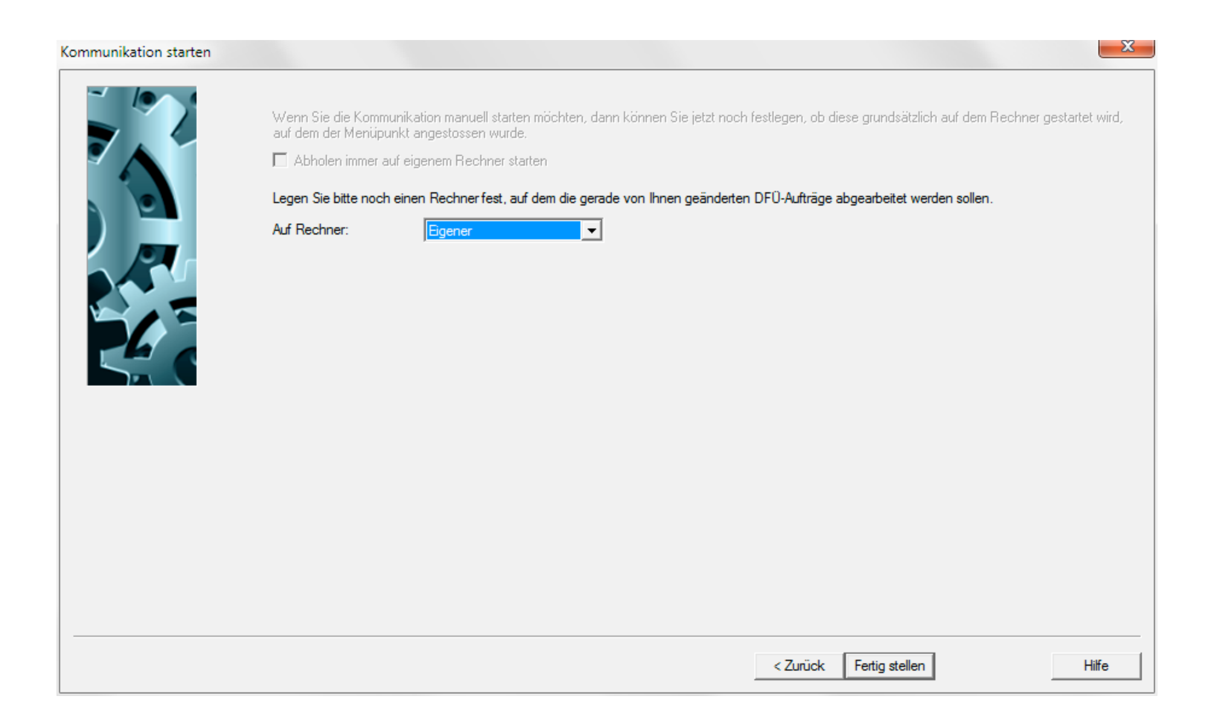


3 **Kommunikation starten**

Wenn Sie auf der ersten Seite festgelegt haben, dass Sie die Kommunikation manuell starten möchten, können Sie hier noch festlegen, dass die definierten Aufträge zum **Abholen immer** nur **auf** dem **eigenen Rechner** ge**start**et wer**den** dürfen. Markieren Sie dazu das entsprechende Kontrollkästchen. Andernfalls können Sie hinter "**Auf Rechner:**" innerhalb eines Netzwerkes einen Rechner festlegen, auf dem die DFÜ-Aufträge abgearbeitet werden sollen (ebenso bei automatischem Rundruf).

Beenden Sie diesen letzten Schritt über die Schaltfläche [***Fertig stellen***].
Anschließend werden DFÜ-Aufträge mit dem Ordnungsbegriff "AUTOMAT" aus Ihren Angaben generiert.





Über die Schaltfläche [**< *Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.



Funktion "Informationen von Bank(en) abholen" / Rundruf (manuell)

Das **manuelle** Starten der Rundruf-Funktion zur Abarbeitung Ihrer definierten Abholaufträge erfolgt vom Grundbildschirm aus über das folgende Icon aus der Symbolleiste:

 oder .

Stehen mehrere sogenannte Auftragsstapel für manuell zu startende Kommunikation zur Verfügung, so werden diese nach Anklicken des Icons zur Auswahl angeboten, sofern sie mindestens einen gerade fälligen Abholauftrag enthalten.

 **Bitte beachten Sie:**

Enthält ein Stapel ausschließlich Aufträge, die in Bezug auf Ausführungszeit und/oder -rhythmus nicht fällig sind (z. B. weil der Zeitpunkt des manuellen Aufrufs außerhalb eines vorgegebenen Zeitfensters liegt), wird dieser Stapel nicht zur Auswahl angeboten.

Existiert kein manuell auszuführender Auftragsstapel mit mindestens einem fälligen Abholauftrag, wird in der Auswahlliste "Kein Satz gefunden." angezeigt.

Wählen Sie den gewünschten Auftragsstapel mittels Mausklick aus und bestätigen Sie mit [***OK***]. Nur die fälligen Aufträge des ausgewählten Stapels werden dann ausgeführt.

Anschließend werden alle Aufträge z. B. mit Rhythmus "Einmal", bei denen die Kommunikation manuell durchgeführt werden soll (entsprechendes Kontrollkästchen markiert, s. o.), sofort ausgeführt und danach unabhängig vom Ergebnis auf den Status "Wartet auf DFÜ" gesetzt. Damit können sie jederzeit wieder manuell gestartet werden.
(Wurde zusätzlich ein Termin für die 1. Übertragung angegeben, werden die Aufträge nicht sofort, sondern erst zu dem angegebenen Termin ausgeführt.)

Aufträge mit Rhythmus "Jedesmal (tägl. bis erfolgreich)" können solange per Icon gestartet werden, bis sie einmal am aktuellen Tag erfolgreich waren.

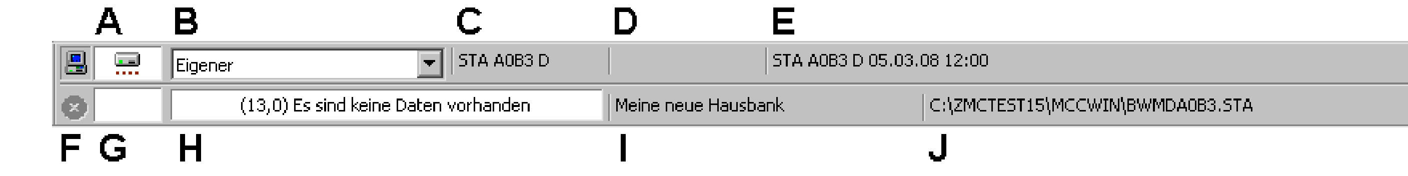


5.3 DFÜ ausführen

DFÜ-Prozesse werden sinnvollerweise im Hintergrund ausgeführt, damit der Anwender - auch wenn die DFÜ läuft - mit anderen Funktionen des Programms arbeiten kann.

Zur Ausführung der im Datei-Manager eingestellten Kommunikations-Aufträge verwenden Sie die Schaltflächen [***Auftrag ausführen***] bzw. [***Alle fälligen Aufträge ausführen***].

Die Ausführung von Kommunikations-Aufträgen erfolgt automatisch, wenn ein entprechender Eintrag im Datei-Manager vorhanden ist und die **DFÜ-Leiste** auf dem Bildschirm zu sehen ist (schaltbar über Menü -Ansicht-).



Teile der DFÜ-Leiste und was sie anzeigen bzw. was sie bewirken:

A: Aktueller Status der Kommunikations-Verarbeitung in Form von Symbolen (Wartezustand:  , DFÜ aktiv: , DFÜ-Nachbearbeitung:)

B: Rechner, dessen Kommunikations-Status angezeigt werden soll

C: Name des gerade ausgeführten DFÜ-Auftrags

D: Name des DFÜ-Moduls, das gerade aktiv ist (DFÜ-Verfahren, z. B. MCFT, EBICS)

E: Nächster zur Ausführung anstehender DFÜ-Auftrag

F: Stopp-Button zum Abbruch des aktuell ausgeführten DFÜ-Auftrags

G: Symbolanzeige zum Zustand des aktuell ausgeführten Kommunikations-Auftrags (z. B. Verbindungsaufnahme, Übertragungsrichtung, Verbindungsabbruch): 

H: Fortschrittsanzeige des aktuell ausgeführten DFÜ-Auftrags / Ergebnis

I: Name der Bank(parameterdatei), zu der (aktuell) eine DFÜ ausgeführt wird / wurde

J: Name der Datei zum (aktuell) ausgeführten DFÜ-Auftrag

Über ein Listenfeld (Feld B) können Sie, falls Sie in einem Netzwerk arbeiten, den Rechner bestimmen, dessen DFÜ-Status in der DFÜ-Leiste angezeigt werden soll.

Stehen **keine** DFÜ-Aufträge konkret zur Ausführung an, so zeigt die **DFÜ-Leiste** (wenn über -Ansicht- / -DFÜ-Leiste aktiviert) an, dass sich derzeit kein DFÜ-Auftrag in Bearbeitung befindet (**Modus "wartend"**, vgl. obige Leiste). Darüber hinaus entnehmen Sie der DFÜ-Leiste, welcher DFÜ-Auftrag wann als nächstes bearbeitet werden wird (Feld E).

Stehen DFÜ-Aufträge konkret zur Ausführung (Ausführungszeitpunkt bei automatischen Aufträgen erreicht) an bzw. wurden DFÜ-Aufträge gestartet, so wechselt die DFÜ-Leiste sofort in den **"aktiven" Modus**:

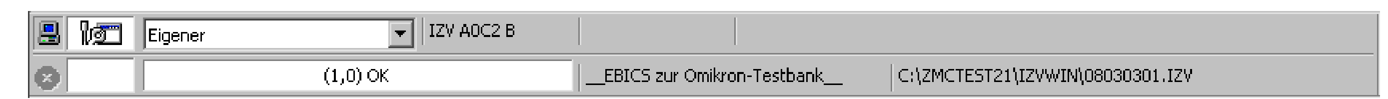




Der ersten Zeile DFÜ-Leiste können Sie dann die folgenden Informationen entnehmen: Name des gerade ausgeführten DFÜ-Auftrags sowie Name des verwendeten DFÜ-Verfahrens. Über die Felder G und H in der zweiten Zeile erhalten Sie weitere Informationen über den Stand der Verarbeitung des Auftrages.

Mit Hilfe des Stopp-Buttons ( ) in der zweiten Zeile können Sie die gerade in Ausführung befindliche Datenfernübertragung abbrechen.
Das Anklicken des Stopp-Buttons bedeutet, dass nur noch der gerade in Ausführung befindliche Auftrag per DFÜ übertragen wird. Alle nachfolgenden Aufträge werden nicht bearbeitet.
Das System zeigt entweder die Meldung "Abbruch durch den Benutzer" oder im Falle einer Erstellung des Startblockes im Rahmen einer ZVDFÜ-Übertragung "Fehler beim Erstellen der Startnachricht".

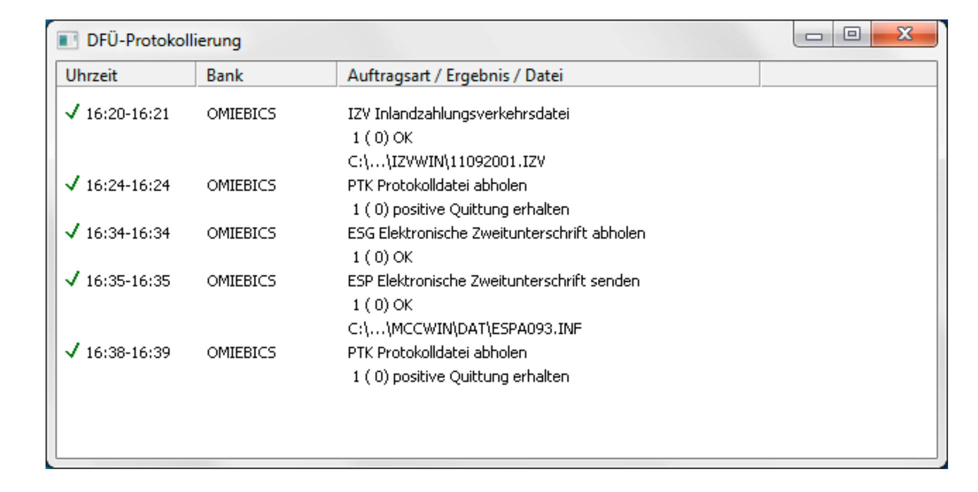
Die Datenfernübertragung bleibt aktiv, solange fällige DFÜ-Aufträge vorhanden sind. Nach Abschluss der DFÜ wechselt die DFÜ-Leiste in den **Modus der "DFÜ-Nachbearbeitung"**:



Sind alle fälligen Aufträge ausgeführt, wird die Datenfernübertragung wird mit entsprechenden Antwortcodes und Hinweistexten beendet (z. B. "(1,0) Auftrag wurde erfolgreich abgeschlossen!"). Nach der Übertragung bleibt das Ergebnis der letzten Verbindung zur Kontrolle in der zweiten Zeile stehen.

Sobald der Zeitpunkt zur Ausführung eines automatischen Kommunikationsauftrages erreicht ist, startet die Datenfernübertragung erneut.

Haben Sie über das Menü -Ansicht- die sogenannte **DFÜ-Protokollierung** aktiviert, werden in einem separaten Fenster die seit Programmstart ausgeführten DFÜ-Aufträge angezeigt. Das Fenster bleibt immer als oberstes Fenster offen und zeigt einige Informationen des DFÜ-Protokolls an. Erfolgreich abgeschlossene Aufträge sind mit einem Häkchen ( ) gekennzeichnet. Bei Fehlermeldungen warnt Sie ein entspechendes Symbol ( ).



Wurden Übertragungen nicht erfolgreich durchgeführt, können Sie weitere Einzelheiten dem DFÜ-Protokoll (s. Kapitel 6.10: *Protokolle*) entnehmen.



Besonderheiten bei Nutzung des Kommunikationsverfahrens ZVDFÜ:

Bei Einsatz des DFÜ-Verfahrens **ZVDFÜ** wird im ersten Schritt auf Kundenseite ein sogenannter **Startblock** erstellt. Dieser Startblock enthält neben anderen Daten den **K**unden-**Z**ahlungs**v**erkehrsschlüssel (**KZV**).

Dieser Schlüssel wird im Rahmen jeder ZVDFÜ-Übertragung neu berechnet. Während der Schlüsselberechnung sehen Sie den Hinweis "**KZVUP Berechnung**".Der KZV ist ein dynamischer Schlüssel, der für jeden Teilnehmer individuell über das **Public-Key-Exchange**-Verfahren nach **Diffie/Hellman** berechnet wird. Der Schlüssel selbst wird nicht übertragen, sondern bildet nur den Startwert zur späteren **Neuberechnung** des **KZV**. Nur die errechnete Änderung des KZV wird an die Bank übertragen. Der Startblock wird vom Bankrechner decodiert.

Nach jeder fehlerfreien Datenübertragung findet ein Schlüsselwechsel auf Bank- und Kundenseite statt. In diesem Fall ist eine Neuberechnung des KZV erforderlich.

Der KZV wird kundenseitig nach einer Neuberechnung in verschlüsselter Form in die entsprechende Bankparameterdatei geschrieben. Erfolgt der Zugriff auf die Bankparameterdatei über Diskette, so ist es unbedingt erforderlich, dass diese **Diskette** bis zum Ende der **Neuberechnung** des **KZV** im Diskettenlaufwerk verbleibt.
Die Neuberechnung ist abgeschlossen, wenn der Hinweis "KZVNEU Berechnung" im unteren Bereich des DFÜ-Fensters erloschen und damit der Schlüssel auf die Bankdiskette zurückgeschrieben wurde.



5.4 Antwort-Codes

Die Bedeutung der Antwort-Codes ist abhängig vom verwendeten DFÜ-Verfahren.

Es wird unterschieden zwischen:

- ZVDFÜ- (MCFT)-Antwort-Code
- FTAM-Antwort-Code
- FTP-Antwort-Code
- EBICS-Antwort-Codes

In der folgenden Auflistung ist zunächst die Bedeutung der vom Bankrechner ausgegebenen Antwort-Codes erläutert. Es schließt sich eine kurze Beschreibung zur möglichen Fehlerursache an.



Die mit nebenstehendem Symbol gekennzeichneten Zeilen enthalten einen Vorschlag zur Fehlerbehebung.



Bei nebenstehendem Symbol sollten Sie den für Ihre Betreuung zuständigen Systemberater Ihrer Bank anrufen und ihm die Fehlermeldung mitteilen.



Es existieren die folgenden **ZVDFÜ-Antwort-Codes**:

AC Bedeutung, Fehlerursache und -behebung

0 **Die Übertragung wurde noch nicht durchgeführt**
Es wurde bisher noch keine Übertragung durchgeführt oder die Übertragung wurde evtl. aufgrund einer schlechten Leitungsqualität unterbrochen.


Führen Sie die Übertragung durch oder wiederholen Sie sie.

1 **Die Übertragung wurde erfolgreich durchgeführt**
Die Übertragung wurde ohne Fehler durchgeführt, es ist keine weitere Aktion Ihrerseits notwendig.

Bei einem Auftrag mit verteilten Unterschriften können im Rahmen dews MCDFÜ-Prozesses) noch Subantwortcodes mitübertragen werden, die das Ergebnis weiter spezifizieren, und zwar:
-1 Weitergeleitet zur Zweitunterschrift:
Die Unterschrift war korrekt, aber noch nicht ausreichend. Die Datei wird anderen zur Zweitunterschrift berechtigten Kunden zur Verfügung gestellt.
-2 Unterschriften noch nicht ausreichend:
Kann nur beim Senden einer Zweitunterschrift auftreten (Sessiontyp ESP). Die Unterschrift wurde korrekt angenommen, zur Vervollständigung muss aber noch auf die Zweitunterschrift eines anderen Kunden gewartet werden.
-3 Datei bereits verarbeitet:
Kann nur beim Senden einer Zweitunterschrift auftreten (Sessiontyp ESP). Die Unterschrift wurde korrekt angenommen, die Datei aber bereits von anderen Kunden vollständig unterschrieben. Die gesendete Unterschrift wird auf der Bankseite verworfen.
-4 Letzte Zweitunterschrift nicht ausreichend

2* **Die Teilnehmernummer ist nicht registriert**


Ihre Teilnehmernummer wurde auf dem Bankrechner (aus Versehen) gelöscht.

3* **Transaktionsnummer ist falsch**


Der Bankrechner erwartet andere Informationen als diejenigen, die übersandt wurden.

4 **Die Übertragung wurde vom Bankrechner abgelehnt**
Es wurde auf dem Bankrechner seit einiger Zeit nicht mehr die Funktion -Dateien abholen- durchgeführt. Der für Sie reservierte "Speicherplatz" ist belegt.


Wiederholen Sie die Übertragung zu einem späteren Zeitpunkt.

5* **Die Teilnehmernummer ist gesperrt**


Ihre Teilnehmernummer wurde von Seiten der Bank gesperrt. Sie können deshalb keine Dateien mehr an den Bankrechner übertragen bzw. von dort abholen. Sie benötigen eine neue Bankdiskette mit einer neuen Bankparameterdatei (BPD-Datei).

6 **Der Teilnehmereintrag ist gerade belegt**
Der Bankrechner führt z. B. gerade die Funktion -Dateien abholen- durch, mit der wieder "Speicherplatz" für die von Ihnen übersandten Dateien zur Verfügung gestellt wird.


Wiederholen Sie die Übertragung zu einem späteren Zeitpunkt.



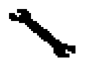
7* **Der Sessiontyp ist unzulässig**



Der Bankrechner ist nicht in der Lage, den von Ihnen übersandten Datentyp zu verarbeiten.

8* **Es wurde bisher kein Installationslauf durchgeführt**

Bevor Sie zum ersten Mal eine Datenübertragung durchführen, muss eine Installation erfolgen. Mit der Installation melden Sie dem Bankrechner, dass er ab sofort mit Datenübertragungen Ihrerseits zu rechnen hat. Ohne eine Installation lehnt der Bankrechner jeden Übertragungsversuch ab.



Führen Sie eine Passwort-Initialisierung durch (INI) bzw. verwenden Sie den Erstzugangsassistenten, um die Initialisierungsaufträge für die ZVDFÜ- bzw. FTAM-Banken zu erstellen.

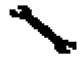
9 **Interner Fehler: siehe Fehlerprotokoll**



Die Plattenkapazität des Bankrechners reicht nicht mehr aus, um die von Ihnen übertragenen Daten zu speichern. Auf der Bankseite muss eine Reorganisation der Festplatte vorgenommen werden.

10* **Die Datei wurde bereits übertragen**

Sie haben versucht, eine Datei zu übertragen, die Sie schon zu einem früheren Zeitpunkt an Ihre Bank gesandt haben.



Prüfen Sie bitte, ob sie die Datei nur aus Versehen noch einmal übertragen haben oder ob Sie wirklich eine nochmalige Übertragung der Datei vornehmen wollen. Wenn Sie die Datei wirklich noch einmal übertragen wollen, rufen Sie den für Sie zuständigen Systemberater der Bank an und teilen ihm Ihren Wunsch mit. Er wird das weitere veranlassen.



Haben Sie jedoch nur aus Versehen die Übertragung der Datei initialisiert, ist keine weitere Aktion Ihrerseits mehr erforderlich.

11 **Die Übertragung wurde vom Bankrechner abgebrochen**

Die Übertragung wurde evtl. aufgrund einer schlechten Leitungsqualität unterbrochen.



Wiederholen Sie die Übertragung bitte zu einem späteren Zeitpunkt.

12 **Die Checksumme ist falsch**

Die Daten sind evtl. aufgrund einer schlechten Leitungsqualität "verstümmelt" beim Bankrechner eingegangen.



Wiederholen Sie die Übertragung bitte zu einem späteren Zeitpunkt.

13 **Es sind keine Daten vorhanden**

Der Bankrechner verfügt über (noch) keine Daten, die von Ihnen abgeholt werden können.



Wiederholen Sie den Abholversuch bitte zu einem späteren Zeitpunkt.



14* **Sie haben keine Übertragungsberechtigung für dieses Konto**



Von Seiten der Bank wurde die Übertragungsberechtigung für ein bestimmtes Konto gelöscht.

15* **Keine Berechtigung für diesen Sessiontyp**



Von Seiten der Bank wurde die Übertragungsberechtigung für einen bestimmten Datentyp (DTAUS-Datei, DTAZV-Datei, Unterschriftsdatei usw.) gelöscht bzw. noch nicht erteilt.

16 **Fehler bei der logischen Prüfung der Nachrichten**

Die Daten sind evtl. aufgrund einer schlechten Leitungsqualität "verstümmelt" beim Bankrechner eingegangen.



Wiederholen Sie die Übertragung bitte zu einem späteren Zeitpunkt.

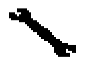
17* **Teilnehmer wegen 3 Fehlversuchen gesperrt**



Die Zugangsberechtigung zum Bankrechner wurde gesperrt, nachdem auf Iher Seite dreimal hintereinander eine falsche Benutzer-PIN zur Initialisierung einer Übertragung / eines Abholvorganges eingegeben wurde. Sie können deshalb keine Dateien mehr an den Bankrechner übertragen bzw. von dort abholen. Sie benötigen eine neue Bankdiskette mit einer neuen Bankparameterdatei (BPD-Datei).

18* **Tagesdatum Kundenrechner ungültig**

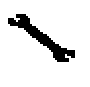
Das Systemdatum Ihres Rechners weicht mehr als 2 Tage in der Zukunft oder mehr als 14 Tage in der Vergangenheit vom Systemdatum des Bankrechners ab.



Kontrollieren Sie auf Betriebssystemebene mit dem DOS-Befehl "date" das Systemdatum. Korrigieren Sie das Systemdatum und wiederholen Sie anschließend die Übertragung.

19 **Abbruch durch den Benutzer**

Die Speicherkapazität Ihres Rechners reicht nicht mehr aus, die vom Bankrechner abgeholten Daten auf die Festplatte zu schreiben.



Führen Sie eine Reorganisation Ihrer Datenbanken durch, indem Sie z. B. über den Menüpunkt -Verwaltung- / -Reorganisation- aufrufen (s. Basismodul-Kapitel 7.3: *Datenbank-Reorganisation*) oder indem Sie nach Beenden des Programms durch Sicherung von Dateien auf externe Speichermedien weiteren "Speicherplatz" auf Ihrer Festplatte schaffen.

20 **Abbruch mit ESC**

Die Übertragung wurde durch Eingabe von <**ESC**> abgebrochen.

21* **Die Datei wurde manipuliert (Checksumme)**



Die Überprüfung durch den Bankrechner ergab, dass die übertragene Datei auf der Kundenseite nach dem Einstellen in einen DFÜ-Auftrag manipuliert wurde.



Ersetzen Sie die manipulierte Datei und wiederholen Sie anschließend die Übertragung.



22 **Fehler beim Schreiben der Datei lokal**

Beim Schreiben der abgeholten Datei auf Ihre Festplatte trat ein Fehler auf.



Überprüfen Sie Ihre Festplatte und wiederholen Sie anschließend die Übertragung.

23* **Fehler beim Entschlüsseln der Startnachricht**

Die von Ihnen eingetragene Benutzer-PIN ist nicht mehr gültig, da zuvor eine Änderung der Benutzer-PIN durchgeführt wurde.



Wiederholen Sie bitte die Übertragungs- / Abholversuche, nachdem Sie die derzeit gültige Benutzer PIN eingetragen haben.

25 **Teilnehmer noch nicht freigeschaltet**

Die Übertragung wurde abgelehnt, weil Sie auf Bankrechnerseite noch nicht freigegeben wurden.



Erkundigen Sie sich bei dem Systemberater Ihrer Bank, warum die Freigabe Ihres Teilnehmerdatensatzes bislang nicht erfolgte.

27 **Anderer Auftrag mit Bank nicht komplett**

Die Übertragung wurde abgelehnt, da Ihr Kundensystem eine vorangegangene Kommunikation mit dem betreffenden Bank-Server nicht vollständig abgeschlossen hat.



Bevor andere Dateien übermittelt werden können, müssen Sie zuerst den unvollständigen Auftrag, der mit Antwortcode 29 gekennzeichnet ist, erneut ausführen, damit er komplett beendet werden kann. Danach wird die Sperre dieser Bank automatisch aufgehoben.

29 **Abstimmung Bank fehlt, bitte wiederholen**

Die Übertragung dieses Auftrages wurde nicht vollständig abgeschlossen, weil die Verbindung abgebrochen ist, bevor die Bestätigung des Banksystems empfangen wurde. Das Banksystem kann die Verarbeitung also korrekt abgeschlossen oder ebenfalls einen Abbruch registriert haben. Der Status dieses Auftrages ist offen.



Bitte führen Sie diesen Auftrag erneut aus, damit er komplett beendet werden kann. Hierbei werden die Daten zunächst nicht erneut übertragen, sondern der Status dieses Auftrages bei der Bank abgefragt. Hat das Banksystem die Daten angenommen, wird der Status auf AC 1 gesetzt und der Auftrag ist positiv beendet. Hat das Banksystem die Daten nicht erhalten, wird der AC 11 gesetzt und die Übertragung wiederholt.

Würde die betroffene Zahlungsdatei mit einem neuen DFÜ-Auftrag nochmals übertragen, könnte dies zu doppelter Verarbeitung bei der Bank führen. Deshalb wird die betroffene Bank-Parameter-Datei so lange gesperrt, bis der unvollständige Auftrag komplett abgearbeitet ist. Andere Aufträge an diese Bank werden deshalb während dieses Zeitraumes mit AC 27 abgebrochen.



Achtung:
Wenn bei der erneuten Ausführung des unvollständigen Auftrages das Banksystem nicht erreicht werden kann, bleibt der AC 29 bestehen. Sie können nicht sicher sein, dass der Auftrag bei der Bank NICHT eingegangen ist. Bevor Sie den Auftrag auf anderem Wege ausführen, sprechen Sie mit Ihrer Bank. Nur so können Doppelausführungen sicher ausgeschlossen werden!



Folgende ZVDFÜ-Antwort-Codes kommen nur vor, wenn das Kommunikationsverfahren ZVDFÜ mit Elektronischer Unterschrift (= **MCFT**) verwendet wird:

AC	Bedeutung
28	**Noch nicht alle Unterschriften vorhanden** Die Zahl der notwendigen Unterschriften wurde noch nicht erreicht.
30*	**Neuer Public Key noch nicht freigegeben** Sie haben einen Sessiontyp PUB geschickt, dieser wurde aber auf der Bankseite noch nicht mit <Shift> <F8> freigeschaltet.
31*	**Elektronische Unterschrift fehlerhaft** 1. Nach dem Startblock: Das Verifizieren der EU ist fehlgeschlagen. Ursachen: Der Kunde arbeitet mit einem veralteten Keypaar. 2. Nach dem Schlussblock: Hashwert der Datei stimmt nicht. Ursachen: Die gesendete und die unterschriebene Datei stimmen nicht überein.
32*	**Noch kein Public Key vorhanden** Auf der Bankseite ist Ihr Public-Key nicht gespeichert. Das kann daran liegen, dass Sie zwar ein Keypaar generiert, dieses aber noch nicht zur Bank verschickt hat.
33*	**Inkonsistente Unterschriftsdatei** Die Unterschrift ist inkonsistent, weil - der gleiche Teilnehmer mehrfach unterschrieben hat, - der Zeitstempel der Originaldatei unterschiedlich ist.
34	**Unterschriften nicht ausreichend** Die Zahl der geleisteten Unterschriften ist nicht ausreichend. Hier wird noch ein Subantwortcode übertragen, und zwar: -2 Unterschriftsklassen ungültig In der EU-Datei ist eine nicht ausreichende Kombination der U-Klassen vorhanden; gültig sind (E), (AA) und (AB). -5 Datei muss unterschrieben werden Die Datei wurde ohne EU geschickt, dies wird aber vom Bankrechner verlangt. -6 Teilnehmer darf nicht unterschreiben Der Teilnehmer hat die Unterschriftsklasse N.
35*	**Keine Unterschriftsberechtigung für dieses Konto** Beim Senden der Originaldatei oder der ESP-Datei wird das Konto, für das keine Berechtigung besteht, im DFÜ-Auftrag angezeigt. Es kann auch sein, dass zwar die Berechtigung besteht, aber vielleicht nur für einen Teilnehmer mit nicht ausreichender Unterschriftsklasse.
36	**Reserviert (für interne Steuerungszwecke)**
37*	**Limit überschritten**

Bei Auftreten der mit ***** gekennzeichneten Antwort-Codes werden die entsprechenden DFÜ-Aufträge **nicht** automatisch wiederholt, da es sich in diesen Fällen um schwerwiegende Fehler bzw. Verstöße gegen die Sicherheitsmassnamen von ZVDFÜ/MCDFÜ handelt.



Es existieren die folgenden **FTAM-Antwort-Codes**:

Die Hinweise zur Fehlerursache und -behebung finden Sie unter den einander entsprechenden AC-Nummern der ZVDFÜ-Antwort-Codes.

AC	Bedeutung
0	**Die Übertragung wurde noch nicht durchgeführt**
1	**Auftrag durchgeführt**
2*	**User-ID nicht registriert**
3*	**Falsches Passwort**
5*	**User-ID gesperrt**
7*	**Unzulässige Auftragsart**
8*	**User-ID nicht initialisiert**
9	**Interner Fehler**
13	**(Noch) keine Daten vorhanden, später versuchen**
15*	**Keine Berechtigung für diese Auftragsart**
16	**Formalfehler**
17*	**Sperrung der User-ID nach 3 Fehlversuchen**
24	**Keine Daten vorhanden** Es sind keine Daten für Sie auf dem Bankrechner zum Abholen bereit.
25	**User-ID noch nicht freigegeben**
26*	**Nicht normierter Fehler;** **Auftragswiederholung nicht sinnvoll** Auf Seiten des Bankrechners ist eine Betriebsstörung aufgetreten.
27	**Nicht normierter Fehler;** **Auftragswiederholung sinnvoll** Auf Ihren Datensatz im Bankrechner erfolgte gerade ein Zugriff, z. B. seitens eines HOST-Prozesses.
28	**Negative Bestätigung;** **Auftragswiederholung sinnvoll** **(der ausgegebene Text ist variabel)**
29	**Abbruch der gesamten DFÜ-Verbindung** **(der ausgegebene Text ist variabel)**

Bei Auftreten der mit ***** gekennzeichneten Antwortcodes werden die entsprechenden DFÜ-Aufträge **nicht** automatisch wiederholt, da es sich in diesen Fällen um schwerwiegende Fehler bzw. Verstöße gegen die Sicherheitsmassnamen von FTAM handelt.

Im Rahmen der **Verschlüsselung** werden zusätzlich banksystemseitig die nachfolgend aufgeführten Antwortcodes ausgegeben, die kundenseitig die entsprechend beschriebenen Aktionen auslösen, sofern diese im FTAM-Remote-Dateinamen die Versionskennung des Anwendungsprotokolles "A3" verwendet. (Ältere Kundensysteme, die mit der Versionskennung "A2" arbeiten, erhalten diese Antwortcodes grundsätzlich nicht.)

AC	Bedeutung
50	**Aktion erfolgreich - Neue Bankparameterdaten abholen**
51	**Verschlüsselungscode mit Bank muss aktualisiert werden (Auftragsart VPB)**
52	**Daten müssen verschlüsselt abgeholt werden**
53	**Daten müssen unverschlüsselt abgeholt werden**
54	**Verschlüsselungscode muss neu verschickt werden (VPK)**
55	**User nicht EU-berechtigt**
56	**Verschlüsselungscode noch nicht freigegeben**

Die Bedeutung der Antwort-Codes finden Sie in Kapitel 4.5.2: *DFÜ-Returncodes im Rahmen der Verschlüsselung* beschrieben.



Zusätzlich zu den **ebenso für FTP geltenden Antwort-**Codes des FTAM-Protokolls gibt es folgende Returncodes für die Online EU-Prüfung:

AC	Bedeutung
60	**EU angegebener Hashwert ok**
61	**EU angegebener Hashwert nicht ok**
62	**EU ok**
63	**EU nicht ok, siehe Protokolldatei**
64	**EU nicht geprüft, siehe Protokolldatei**
65	**Daten noch nicht bereit, Pollingrate**
66	**Fehler Verschlüsselungs-Version** Sie versuchen, mit einer anderen als der aktuellen Version des Bankschlüssels zu übertragen. Sie werden durch den Systemberater Ihrer Bank aufgefordert, den aktuellen VPB abzuholen.
67	**Fehler Zeitstempel** Der von Ihnen generierte Auftrag liegt nicht im Zeitfenster des Bankrechners, d.h. er ist zu alt oder mit einem zukünfigen Datum erstellt worden.



Für **EBICS** ist eine neue Systematik 6-stelliger **Returncodes** definiert worden. Die beiden ersten Ziffern bezeichnen die Fehlerklasse:

Fehlerklasse	Bedeutung	Auswirkung auf laufende Transaktion
00	Information	keine
01	Hinweis	keine
03	Warnung	keine
06	Fehler (behebbar)	keine bzw. Erhöhung des Recovery-Zählers
09	Fehler (nicht behebbar)	Abbruch

Dahinter folgt eine Ziffer für das EBICS-Kennzeichen:

EBICS-Kennzeichen	Bedeutung
0	kein EBICS-spezifischer Returncode (außer "EBICS_OK")
1	EBICS-spezifischer Returncode

Anschließend folgt eine Ziffer als Kennzeichen der Untergruppe:

Untergruppe	Bedeutung
0	keine spezifische Untergruppe
1	Transaktionsverwaltung (technisch)
2	Schlüsselmanagement (fachlich)
3	Vorabprüfung (fachlich)

Die beiden letzten Ziffern dienen zur Kennzeichnung des spezifischen Fehlercodes.

Diese EBICS-Returncodes werden auf die bekannten Antwortcodes abgebildet, damit die Nachverarbeitung möglichst wenig beeinflusst wird. Der EBICS-Kurztext (soweit definiert) und der zugehörige symbolische Name des EBICS-Codes werden in den Textzeilen im Dateimanager und im Protokoll angezeigt.

Bei Fehlerklasse 06 kann die Transaktion nach Behebung des Fehlers fortgeführt werden. Die allgemeingültige Maßnahme lautet in diesem Fall Fortsetzen der Transaktion nach Behebung der Fehlerursache.

Bei Fehlerklasse 09 werden die Transaktionen bankseitig abgebrochen. Die allgemeingültige Maßnahme lautet in diesem Fall Wiederholen der gesamten Transaktion nach Behebung der Fehlerursache.

Die nachfolgenden Tabellen, die für einzelne Fehlercodes spezielle Maßnahmen enthalten, sind für jeden EBICS-Returncode (RC) nach folgendem Schema aufgebaut:

EBICS-RC	Symbolischer Name	**Antwortcode**
	Bedeutung, Ursache	ggf. mögliche Maßnahmen



Technische Return-Codes:

Code	Name	Bedeutung
00 0 0 00	EBICS_OK	**01 OK**
	Bei der Verarbeitung des EBICS-Requests sind keine technischen Fehler aufgetreten.	
01 1 0 00	EBICS_DOWNLOAD_POSTPROCESS_DONE	**01 Positive Quittung erhalten**
	Nach Erhalt einer positiven Quittung wurden serverseitig die abschließenden Arbeiten des Downloads durchgeführt und die EBICS-Transaktion beendet.	
01 1 0 01	EBICS_DOWNLOAD_POSTPROCESS_SKIPPED	**27 Negative Quittung erhalten**
	Nach Erhalt einer negativen Quittung wurde serverseitig die Transaktion beendet, ohne die abschließenden Arbeiten des Downloads durchzuführen.	
01 1 1 01	EBICS_TX_SEGMENT_NUMBER_UNDERRUN	**27 Segmentanzahl unterschritten**
	Die bei der Transaktionsinitialisierung übermittelte Gesamtzahl der Segmente wurde unterschritten.	
03 1 0 01	EBICS_ORDER_PARAMS_IGNORED	**27 Unbekannte Auftragsparameter werden ignoriert**
	Unbekannte Auftragsparameter wurden ignoriert (z. B. wenn OrderParams für Upload angegeben wurden).	
06 1 0 01	EBICS_AUTHENTICATION_FAILED	**27 Authentifikationssignatur fehlerhaft**
	Die Verifikation der Authentifikationssignatur war nicht erfolgreich.	
06 1 0 02	EBICS_INVALID_REQUEST	**27 Nachricht nicht EBICS-konform**
	Die empfangene Nachricht entspricht syntaktisch nicht den EBICS-Vorgaben.	
06 1 0 99	EBICS_INTERNAL_ERROR	**27 Interner EBICS-Fehler**
	Bei der Verarbeitung des EBICS-Requests ist ein interner Fehler aufgetreten.	
06 1 1 01	EBICS_TX_RECOVERY_SYNC	**27 Synchronisation erforderlich**
	Das Wiederaufsetzen der Transaktion erfordert die Synchronisation zwischen Kunden- und Banksystem.	Fortsetzen der Transaktion unter Verwendung des Wiederaufsetzpunktes aus der EBICS-Response des Banksystems.
09 1 0 02	EBICS_INVALID_USER_OR_USER_STATE	**02 Teilnehmer unbekannt oder Teilnehmerzustand unzulässig**
	Entweder ist der Einreicher des Auftrags dem Banksystem nicht bekannt, oder der im Banksystem gespeicherte Teilnehmerzustand des Einreichers ist unzulässig bezüglich der Auftragsart.	
09 1 0 03	EBICS_USER_UNKNOWN	**02 Teilnehmer unbekannt**



	Der Einreicher des Auftrags ist dem Banksystem nicht bekannt.	
09 1 0 04	EBICS_INVALID_ USER_STATE	**02 Teilnehmerzustand unzulässig**
	Der im Banksystem gespeicherte Teilnehmerzustand des Einreichers ist unzulässig bezüglich der Auftragsart.	
09 1 0 05	EBICS_INVALID_ORDER_TYPE	**07 Auftragsart unzulässig**
	Die Auftragsart ist unbekannt oder nicht zur Verwendung bei EBICS zugelassen.	
09 1 0 06	EBICS_UNSUPPORTED_ORDER_TYPE	**07 Auftragsart nicht unterstützt**
	Die gewählte Auftragsart ist bei EBICS optional und wird vom Kreditinstitut nicht unterstützt.	
09 1 0 07	EBICS_DISTRIBUTED_SIGNATURE_AUTHORISATION_FAILED	**09 Teilnehmer hat keine Unterschriftsberechtigung** d. h. Verifikation fehlerhaft
	Der Teilnehmer hat keine Unterschriftsberechtigung für den referenzierten Auftrag in der VEU-Verwaltung.	
09 1 0 08	EBICS_BANK_PUBKEY_UPDATE_REQUIRED	**66 Bankschlüssel ungültig**
	Die öffentlichen Bankschlüssel, über die der Teilnehmer verfügt, sind ungültig.	Abholung der aktuellen Bankschlüssel mittels HPB
09 1 0 09	EBICS_SEGMENT_SIZE_EXCEEDED	**26 Segmentgröße überschritten**
	Die festgelegte Größe eines Upload-Auftragsdaten-segmentes (bei H002: 1 MB) wurde überschritten.	
09 1 0 10	EBICS_INVALID_XML	**26 XML nicht valide gemäß EBICS-XML-Schema**
	XML-Validierung gegen EBICS-Schema fehlgeschlagen oder XML nicht wohlgeformt.	
09 1 1 01	EBICS_TX_UNKNOWN_TXID	**27 Transaktions-ID ungültig**
	Die gelieferte Transaktions-ID ist ungültig.	Wenn das Problem beim Recovery mit Aufsetzpunkt vor dem letzten Block auftritt: Wiederholung mit neuer Transaktions-ID Wenn das Problem beim Recovery mit Aufsetzpunkt letzter Block auftritt: 64 EU nicht geprüft, siehe Protokolldatei
09 1 1 02	EBICS_TX_ABORT	**27 Transaktion abgebrochen**
	Die Transaktion wurde serverseitig abgebrochen, da ein Wiederaufsetzen der Transaktion nicht unterstützt wird oder aufgrund eines zu hohen Recovery-Zählers nicht mehr möglich ist.	



09 1 1 03	EBICS_TX_MESSAGE_REPLAY Ein Nachrichten-Replay wurde erkannt (Nonce-Timestamp-Paar doppelt).	**26 Nachrichten-Replay**
09 1 1 04	EBICS_TX_ SEGMENT_NUMBER_EXCEEDED Die Gesamtsegmentzahl aus der Transaktionsinitialisierung wurde überschritten.	**26 Segmentanzahl überschritten**
09 1 1 12	EBICS_INVALID_ORDER_PARAMS Der Inhalt von OrderParams ist inhaltlich ungültig, z. B. Start nach Ende bei StandardOrderParams, fetchOffset bei HVT größer als NumOrderInfos (Gesamtanzahl Einzelauftraginfos im Auftrag).	**26 Ungültige Auftragsparameter**
09 1 1 13	EBICS_INVALID_REQUEST_CONTENT Die empfangene Nachricht entspricht zwar syntaktisch dem EBICS-XML-Schema, entspricht aber semantisch nicht den EBICS-Vorgaben (z. B. IZV-Upload mit UZHNN erfordert NumSegments = 0).	**26 Nachrichteninhalt semantisch nicht EBICS-konform**
09 1 1 17	EBICS_MAX_ORDER_DATA_SIZE_EXCEEDED Upload oder Download einer unzulässig großen Auftragsdatei (z. B. für HVT, IZV, STA).	**26 Das Banksystem unterstützt die angeforderte Auftragsgröße nicht**
09 1 1 18	EBICS_MAX_SEGMENTS_EXCEEDED Das Banksystem unterstützt die spezifizierte Gesamtanzahl der Segmente für den Upload nicht.	**26 Die übergebene Anzahl der Segmente für den Upload ist zu groß**
09 1 1 19	EBICS_ MAX_TRANSACTIONS_EXCEEDED Die im Banksystem für den Kunden konfigurierte maximale Anzahl paralleler EBICS-Transaktionen wurde überschritten.	**26 Maximale Anzahl paralleler Transaktionen pro Kunde überschritten**
09 1 1 20	EBICS_PARTNER_ID_MISMATCH Bei der Überprüfung der eingereichten Unterschriften wurde im UserSignatureData-Dokument eine PartnerID gefunden, die nicht mit der PartnerID des Teilnehmers im Requestheader identisch ist.	**26 Die PartnerID (=KundenID) der EU-Datei stimmt nicht mit der PartnerID (=KundenID) des Einreichers überein**
09 1 1 21	EBICS_INCOMPATIBLE_ORDER_ATTRIBUTE	**26 Das angegebene Auftragsattribut ist nicht kompatibel zum Auftrag im Banksystem**



	Z. B. Auftragsattribut "UZHNN" für Auftrag mit Auftragsattribut "DZHNN", Auftragsattribut "DZHNN" für Auftrag mit Auftragsattribut "UZHNN" oder "OZHNN". auch: Im Banksystem ist bereits eine Datei von diesem Kunden mit derselben Auftragsnummer (z. B. IZV A030) gespeichert.	Nächste Auftragsnummer in der Auftragsartentabelle anpassen und Auftrag erneut versenden.

Fachliche Return-Codes:

00 0 0 00	EBICS_OK	**01 OK**
	Bei der Verarbeitung des EBICS-Requests sind keine fachlichen Fehler aufgetreten.	
01 1 3 01	EBICS_NO_ONLINE_CHECKS	**64 Vorabprüfung nicht unterstützt** d. h. EU nicht geprüft, siehe Protokolldatei
	Die optionale Vorabprüfung wird vom Banksystem nicht unterstützt.	
09 1 0 01	EBICS_DOWNLOAD_SIGNED_ONLY	**26 Banksystem fordert Signatur**
	Das Banksystem unterstützt für den vorliegenden Auftrag nur bankfachlich signierte Download-Auftragsdaten.	
09 1 0 02	EBICS_DOWNLOAD_UNSIGNED_ONLY	**26 Banksystem unterstützt keine Signatur**
	Das Banksystem unterstützt für den vorliegenden Auftrag nur unsignierte Download-Auftragsdaten.	
09 0 0 03	EBICS_AUTHORISATION_FAILED	**15 Keine Berechtigung für diese Auftragsart** d. h. Sessiontyp
	Der Teilnehmer ist nicht zur Einreichung des Auftrags mit der gewählten Auftragsart befugt.	
09 0 0 04	EBICS_INVALID_ORDER_DATA_FORMAT	**26 Formatfehler in Auftragsdaten**
	Die übergebenen Auftragsdaten entsprechen nicht dem festgelegten Format.	
09 0 0 05	EBICS_NO_DOWNLOAD_DATA_AVAILABLE	**24 Derzeit keine Daten verfügbar** d. h. keine Daten vorhanden
	Für die gewählte Download-Auftragsart sind derzeit keine Daten verfügbar.	Download zu einem späteren Zeitpunkt wiederholen
09 0 0 06	EBICS_UNSUPPORTED_REQUEST_FOR_ORDER_INSTANCE	**26 Anfrage für Geschäftsvorfall nicht mögl.**
	Das Banksystem unterstützt für den konkreten Geschäftsvorfall des Auftrags die gewählte Auftragsanfrage nicht.	



09 1 1 05	EBICS_RECOVERY_NOT_SUPPORTED Das Banksystem unterstützt Recovery nicht.	**27 Banksystem unterstützt Recovery nicht**
09 1 1 11	EBICS_INVALID_SIGNATURE_FILE_FORMAT Die übergebenen EU-Dateien entsprechen nicht dem festgelegten Format. Die EU-Datei kann syntaktisch nicht geparst werden (keine bankfachliche Prüfung!).	**33 Formatfehler in EU-Dateien** d. h. inkonsistente Unterschriftsdatei
09 1 1 14	EBICS_ORDERID_UNKNOWN Die übergebene Auftragsnummer ist unbekannt. HVE, HVS, HVD, HVT mit unbekannter Kombination PartnerID (=KundenID) / OrderType / OrderID.	**26 Auftragsnummer unbekannt**
09 1 1 15	EBICS_ ORDERID_ALREADY_EXISTS Die übergebene Auftragsnummer ist bereits vorhanden. Für den Kunden wurde bereits ein Auftrag mit derselben Auftragsnummer eingereicht (Doppeleinreichung).	**26 Auftragsnummer bereits vorhanden**
09 1 1 16	EBICS_PROCESSING_ERROR Bei der Verarbeitung des EBICS-Requests sind sonstige fachliche Fehler aufgetreten. Die Nachricht war korrekt, konnte aber aufgrund eines sonstigen fachlicher Fehlers nicht verarbeitet werden.	**26 Sonstige fachliche Fehler aufgetreten**
09 1 2 01	EBICS_KEYMGMT_UNSUPPORTED_VERSION_SIGNATURE Die Algorithmenversion des bankfachlichen Signaturschlüssels wird vom Kreditinstitut nicht unterstützt (Auftragsarten INI und PUB).	**26 Ungültige Version bankfachlicher Schlüssel** INI: unterstützte Algorithmenversionen sind den EBICS-Antragsformularen zu entnehmen PUB: zulässige Algorithmenversionen sind den Bankparametern (HPD)zu entnehmen
09 1 2 02	EBICS_KEYMGMT_UNSUPPORTED_VERSION_AUTHENTICATION Die Algorithmenversion des Authentifikationsschlüssels wird vom Kreditinstitut nicht unterstützt (Auftragsarten HIA, HSA und HCA).	**26 Ungültige Version Auth.-Schlüssel** HIA, HSA: unterstützte Algorithmenversionen sind den EBICS-Antragsformularen zu entnehmen HCA: zulässige Algorithmenversionen sind den Bankparametern (HPD) zu entnehmen
09 1 2 03	EBICS_KEYMGMT_UNSUPPORTED_VERSION_ENCRYPTION Die Algorithmenversion des Verschlüsselungsschlüssels wird vom Kreditinstitut nicht unterstützt (Auftragsarten HIA, HSA und HCA).	**26 Ungültige Version Verschl.-Schlüssel** HIA, HSA: unterstützte Algorithmenversionen sind den EBICS-Antragsformularen zu entnehmen HCA: zulässige Algorithmenversionen sind den Bankparametern (HPD) zu entnehmen
09 1 2 04	EBICS_KEYMGMT_KEYLENGTH_ ERROR_SIGNATURE	**66 Ungültige Länge bankfachlicher Schlüssel**



	Die Schlüssellänge des bankfachlichen Signaturschlüssels wird vom Kreditinstitut nicht unterstützt (Auftragsarten INI und PUB).	zulässige Schlüssellängen beim Kreditinstitut erfragen, Schlüssel neu generieren
09 1 2 05	EBICS_KEYMGMT_KEYLENGTH_ERROR_AUTHENTICATION	**66 Ungültige Länge Auth.-Schlüssel**
	Die Schlüssellänge des Authentifikationsschlüssels wird vom Kreditinstitut nicht unterstützt (Auftragsarten HIA, HSA und HCA).	zulässige Schlüssellängen beim Kreditinstitut erfragen, Schlüssel neu generieren
09 1 2 06	EBICS_KEYMGMT_KEYLENGTH_ERROR_ENCRYPTION	**66 Ungültige Länge Verschl.-Schlüssel**
	Die Schlüssellänge des Verschlüsselungsschlüssels wird vom Kreditinstitut nicht unterstützt (Auftragsarten HIA, HSA und HCA).	zulässige Schlüssellängen beim Kreditinstitut erfragen, Schlüssel neu generieren
09 1 2 07	EBICS_KEYMGMT_NO_X509_SUPPORT	**66 Banksystem unterstützt keine X.509-Daten**
	Das Banksystem unterstützt nicht die Auswertung von X.509-Daten (Auftragsarten INI, HIA, HSA, PUB, HCA).	
09 1 3 01	EBICS_SIGNATURE_VERIFICATION_FAILED	**63 Verifikation einer EU fehlgeschlagen** d. h. EU nicht OK
	Die Verifikation einer EU ist fehlgeschlagen. Bei asynchron durchgeführten Aufträgen kann der Fehler während der Vorabprüfung auftreten.	korrekte bankfachliche Signatur erzeugen und Transaktion neu generieren
09 1 3 02	EBICS_ACCOUNT_AUTHORISATION_FAILED	**14 Vorabprüfung Kontorechte fehlgeschlagen** d. h. keine Übertragungsberechtigung für dieses Konto
	Die Vorabprüfung der Kontoberechtigung ist fehlgeschlagen.	
09 1 3 03	EBICS_AMOUNT_CHECK_FAILED	**37 Vorabprüfung Kontolimit fehlgeschlagen** d. h. Limit überschritten
	Die Vorabprüfung des Kontobetragslimits ist fehlgeschlagen.	
09 1 3 04	EBICS_SIGNER_UNKNOWN	**02 Signatur von ungültigem Teilnehmer** d. h. die Teilnehmernummer ist nicht registriert
	Ein Unterzeichner des vorliegenden Auftrags ist kein gültiger Teilnehmer.	
09 1 3 05	EBICS_INVALID_SIGNER_STATE	**25 Signatur mit ungültigem Teilnehmerstatus** d. h. der Teilnehmer ist noch nicht freigeschaltet
	Der Zustand eines Unterzeichners des vorliegenden Auftrags ist nicht zulässig.	



09 1 3 06	EBICS_DUPLICATE_SIGNATURE Der vorliegende Auftrag wurde bereits von dem Unterzeichner unterschrieben.	**33 Der Unterzeichner hat den vorliegenden Auftrag bereits unterschrieben** d. h. inkonsistente Unterschriftsdatei



5.5 Nachverarbeitung / User-Exits

Das Programm unterstützt einen benutzerdefinierbaren **UserCommsExit nach jeder DFÜ**. Für jeden einzelnen Eintrag wird dieser Exit einmal aufgerufen.
Gesucht wird im Verzeichnis ..\MCCWIN oder ..\MCCWIN\PRG entweder die Stapeldatei "UserCommsExit.BAT" bzw. "UserCommsExit.CMD" oder das Programm "UserCommsExit.EXE". Darin können beliebige Scripts ausgeführt werden, z. B. zum Verschieben von Dateien. Ist eine entsprechende Datei vorhanden, dann wird der Exit mit folgenden Parametern aufgerufen (in Klammern die Länge der Felder):

%1="aaa" Dateiart/Sessiontyp (3)
%2="a" Übertragungsrichtung N, P oder G (1)
%3="aaaa" Jobnummer (4)
%4="aaaaa" Jobattribut (5)
%5="aaaaaaaa" BPD-Name (8)
%6="aaaaaaaa" Username extern/UserID (8)
%7="n..n" Antwortcode der DFÜ (1-3)
%8="n..n" Subantwortcode der DFÜ (1-3)
%9="a..a" Antworttext (0-40)
%10="a..a" Antworttext 2.Teil (0-40)
%11="a..a" Dateiname (0-128)
%12="a..a" Zugriffsklasse (0-2)
%13="a..a" Basispfad inklusive Arbeitsverzeichnis (max. 128)
%14="nnnnnnnn" Organisationseinheiten (8) [Zusatzmodul]
%15="nnnnnnnn" Mandant (8) [Zusatzmodul]

Alle Parameter werden in Hochkommas eingeschlossen. Nach Aufruf des Exits wartet das Programm auf die Beendigung des Prozesses und fährt dann in der normalen Verarbeitung fort.

Der Exit wird **ganz am Ende eines Nachverarbeitungslaufes noch einmal global** aufgerufen (also nicht für jede verarbeitete Datei), um zu diesem Zeitpunkt weitere Aktionen (z. B. das Verschieben aller abgeholten STA-Dateien) zu ermöglichen.

In diesem Fall wird nur in Parameter %1 der Inhalt "/A" eingestellt.

UserCommsExit2 kann
- nach der Kommunikation für jede Datei und
- am Ende der Nachverarbeitung einmal für alle Dateien (z. B. für die Weiterleitung von AUSZUG.TXT/UMSATZ.TXT)
mit folgenden Parametern aufgerufen werden:

%1 Verarbeitungskennzeichen (0 = nach der Kommunikation je Datei, 1 = einmal nach Nachverarbeitung)
%2="a..a" Dateiname (0-128)
%3="aaa" Dateiart/Sessiontyp (3)
%4="aaa" Externer Sessiontyp FUL oder FDL (3)
%5="a..a" FileFormat (0-50)
%6="a" Übertragungsrichtung N, P oder G(1)
%7="aaaa" Jobnummer (4)
%8="aaaaa" Jobattribut (5)
%9="aaaaaaaa" BPD-Name (8)
%10="a" Testflag Y oder N (1)
%11="a...a" Username extern/UserID (35)
%12="n..n" Antwortcode der DFÜ (1-3)
%13="n..n" Subantwortcode der DFÜ (1-3)
%14="a..a" Antworttext (0-40)
%15="a..a" Antworttext 2.Teil (0-40)
%16="a..a" Basispfad inklusive Arbeitsverzeichnis (0-128)



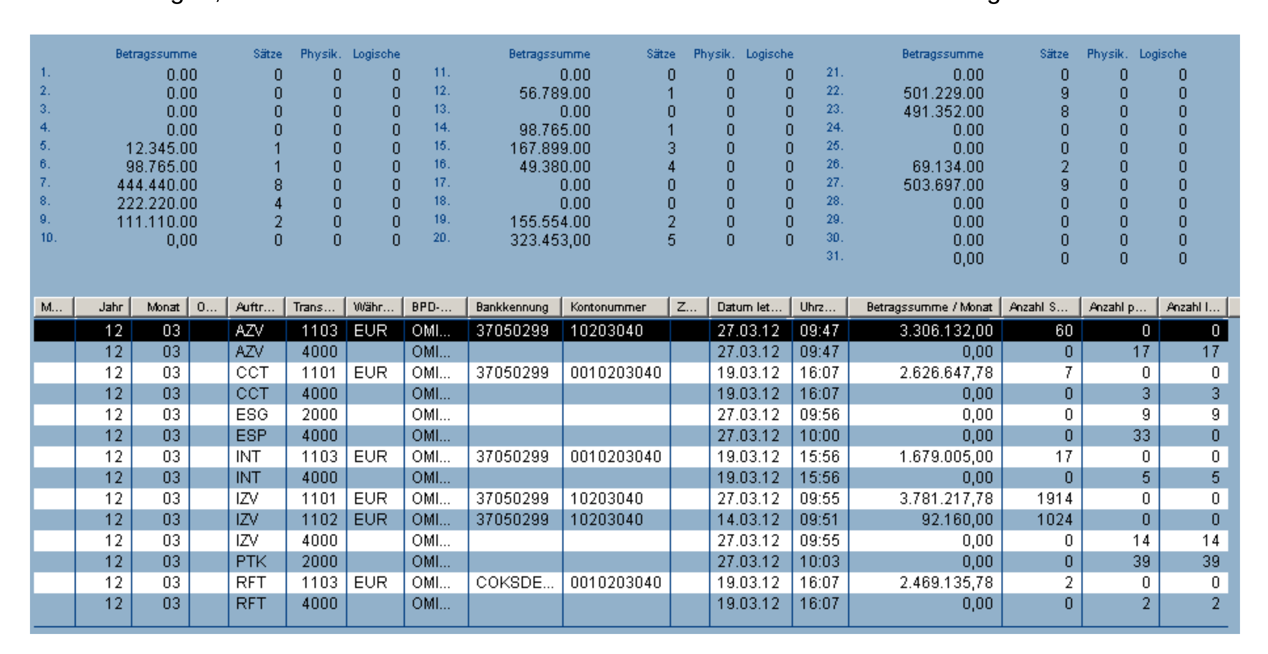
%17="a..a" Zugriffsklasse (0-2)
%18="nnnnnnnn" Organisationseinheiten (8) [Zusatzmodul]
%19="nnnnnnnn" Mandant (8) [Zusatzmodul]
%20="aaaa" Jobnummer extern (4)



5.6 Monatsstatistik (Zusatzmodul)

Über den gleichnamigen Menüpunkt erhalten Sie eine **Monatsstatistik** Ihrer Banktransaktionen.

Für die Monatsstatistik werden mit Hilfe der Format-Subsysteme die Transaktionsdaten der gesendeten Zahlungsverkehrsdateien extrahiert. Bei Austausch anderer Daten wie z. B. Kontoauszügen, Protokollen oder Devisenkursen wird die Anzahl der Dateien festgehalten.



	Betragssumme	Sätze	Physik.	Logische		Betragssumme	Sätze	Physik.	Logische		Betragssumme	Sätze	Physik.	Logische
1.	0.00	0	0	0	11.	0.00	0	0	0	21.	0.00	0	0	0
2.	0.00	0	0	0	12.	56.789.00	1	0	0	22.	501.229.00	9	0	0
3.	0.00	0	0	0	13.	0.00	0	0	0	23.	491.352.00	8	0	0
4.	0.00	0	0	0	14.	98.765.00	1	0	0	24.	0.00	0	0	0
5.	12.345.00	1	0	0	15.	167.899.00	3	0	0	25.	0.00	0	0	0
6.	98.765.00	1	0	0	16.	49.380.00	4	0	0	26.	69.134.00	2	0	0
7.	444.440.00	8	0	0	17.	0.00	0	0	0	27.	503.697.00	9	0	0
8.	222.220.00	4	0	0	18.	0.00	0	0	0	28.	0.00	0	0	0
9.	111.110.00	2	0	0	19.	155.554.00	2	0	0	29.	0.00	0	0	0
10.	0,00	0	0	0	20.	323.453,00	5	0	0	30.	0.00	0	0	0
										31.	0,00	0	0	0

M...	Jahr	Monat	O...	Auftr...	Trans...	Währ...	BPD-...	Bankkennung	Kontonummer	Z...	Datum let...	Uhrz...	Betragssumme / Monat	Anzahl S...	Anzahl p...	Anzahl l...
	12	03		AZV	1103	EUR	OMI...	37050299	10203040		27.03.12	09:47	3.306.132,00	60	0	0
	12	03		AZV	4000		OMI...				27.03.12	09:47	0,00	0	17	17
	12	03		CCT	1101	EUR	OMI...	37050299	0010203040		19.03.12	16:07	2.626.647,78	7	0	0
	12	03		CCT	4000		OMI...				19.03.12	16:07	0,00	0	3	3
	12	03		ESG	2000		OMI...				27.03.12	09:56	0,00	0	9	9
	12	03		ESP	4000		OMI...				27.03.12	10:00	0,00	0	33	0
	12	03		INT	1103	EUR	OMI...	37050299	0010203040		19.03.12	15:56	1.679.005,00	17	0	0
	12	03		INT	4000		OMI...				19.03.12	15:56	0,00	0	5	5
	12	03		IZV	1101	EUR	OMI...	37050299	10203040		27.03.12	09:55	3.781.217,78	1914	0	0
	12	03		IZV	1102	EUR	OMI...	37050299	10203040		14.03.12	09:51	92.160,00	1024	0	0
	12	03		IZV	4000		OMI...				27.03.12	09:55	0,00	0	14	14
	12	03		PTK	2000		OMI...				27.03.12	10:03	0,00	0	39	39
	12	03		RFT	1103	EUR	OMI...	COKSDE...	0010203040		19.03.12	16:07	2.469.135,78	2	0	0
	12	03		RFT	4000		OMI...				19.03.12	16:07	0,00	0	2	2

Die gesammelten Informationen werden monatsweise aggregiert in einer Datenbanktabelle abgelegt. Darüber hinaus werden die Daten getrennt nach

Organisatorischen Kriterien des Betreibers:

- Mandant (soweit das System als ASP-Version betrieben wird)
- Organisationseinheit (soweit das Modul Organisationseinheiten installiert ist)
- Zugriffsklasse (z. B. Lohn/Gehalt)

bzw.

Banktechnischen Kriterien:

- Bankparameterdatei
- Auftragsart (z. B. IZV, AZV)
- Transaktionsart (z. B. Inlandszahlung mit/ohne Unterschrift, Lastschrift mit/ohne Unterschrift)
- Währung
- Bankkennung
- Kontonummer

erfasst.

Getrennt nach den oben genannten Kriterien werden jeweils die folgenden Daten gespeichert:

- Datum und Uhrzeit des letzten Datenaustauschs
- Betragssumme pro Monat
- Anzahl Transaktionen (Sätze) pro Monat
- Anzahl Sammler (physikal. Dateien) pro Monat
- Anzahl Dateien (log. Dateien) pro Monat



Dabei werden die vier letzten Kriterien auch für jeden Tag im Monat registriert, damit bei Bedarf Spitzenzeiten ermittelt werden können.

Für jede der oben beschriebenen Kriterien-Kombinationen wird ein Summensatz je Monat (in der Datensatzliste der Datenbankübersicht) sowie innerhalb des Monats die Tagesstatistik (im Anzeigebereich der Datenbankübersicht) angezeigt.

Nach jedem Kriterium oder nach Kombinationen hiervon kann selektiert und damit genau die gewünschte Information herausgefiltert werden. Dies geschieht entweder mit der Schnellselektionsleiste oder mit dem standardisierten Selektionsdialog.

Zusätzlich können die Daten in gruppierte Drucklisten ausgegeben werden.

Für die individuelle Weiterverarbeitung der Statistikdaten können Sie eine Export-Schnittstelle definieren und die Daten dann z. B. in eine CSV-Datei ausgeben.

☞ **Bitte beachten Sie ...**

Standardmäßig werden alle Statistik-Einträge 12 Monate lang vorgehalten. Ältere Einträge werden beim Aufruf der Monatsstatistik gelöscht.

Dieser Aufbewahrungszeitraum kann über einen CSUB.PRO-Eintrag eingestellt werden:
STATISTIK_VERWAHRDAUER nnn

Dieser Eintrag gibt die Verwahrdauer in Monaten an. Ein Eintrag von '1' würde z. B. am 1.3.2012 alle Einträge aus dem Januar 2012 und früher aus der Datenbank entfernen.



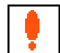
Inhaltsverzeichnis: Kapitel 6

Seite



6 Elektronische Unterschrift

Mit Hilfe der Elektronischen Unterschrift kann die Bank die Identität des Absenders (Kunde) zweifelsfrei ermitteln. Bei Korrektheit aller Elektronischen Unterschriften führt die Bank Ihre Aufträge, wie z. B. Überweisungen, Lastschriften, Auslandszahlungsaufträge usw., aus.


Eine Elektronische Unterschrift zu einem Auftrag kann nur dann erstellt werden, wenn Sie die DFÜ-Verfahren MCFT, FTAM, FTP oder EBICS einsetzen.

Die elektronische Unterschrift stellt eine verschlüsselte Bestätigung zu Ihren Zahlungs- und sonstigen Aufträgen dar.

Die Verschlüsselung besteht aus zwei Teilen; dem "**Private Key**" ("geheimer Schlüssel"), der nur Ihnen bekannt ist, und dem "**Public Key**" ("öffentlicher Schlüssel"), der auch Ihrer Bank zur Verfügung steht.

Die Unterschrift wird mit dem "Private Key" erzeugt und kann daher nur von Ihnen stammen. Anhand des "Public Key" identifiziert die Bank die Richtigkeit und Gültigkeit der Elektronischen Unterschrift.

Das Verfahren beruht auf international anerkannten kryptographischen Algorithmen (RSA-Algorithmus). Die Manipulation oder Fälschung einer Elektronischen Unterschrift ist de facto nicht möglich.

Die beiden zur Durchführung einer Elektronischen Unterschrift benötigten Schlüssel (Private- und Public-Key) werden von Ihnen erstellt (vgl. Kapitel 6.1: *EU-Schlüsselpaar generieren / versenden*). Der geheime Schlüssel wird im Anschluss an eine Verschlüsselung mit einem frei wählbaren EU-Passwort auf einem EU-Medium (s. Kapitel 6.1.5: *Registerkarte Elektronische Unterschrift*) abgespeichert. Der öffentliche Schlüssel muss von Ihnen unter Nutzung der Auftragsart PUB an Ihre Bank verschickt werden.

Änderungen des EU-Passwortes nehmen Sie über den Menüpunkt -Kommunikation- / -EU-Passwort ändern- vor.

Sie unterschreiben Ihre Aufträge mit der Elektronischen Unterschrift entweder im Anschluss an die Erstellung von Aufträgen oder später im Datei-Manager.

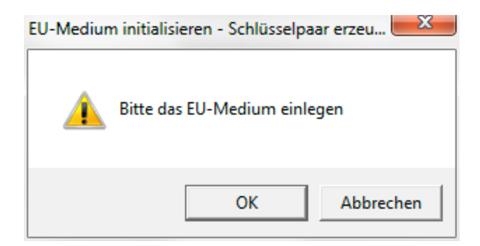


6.1 EU-Schlüsselpaar generieren / versenden

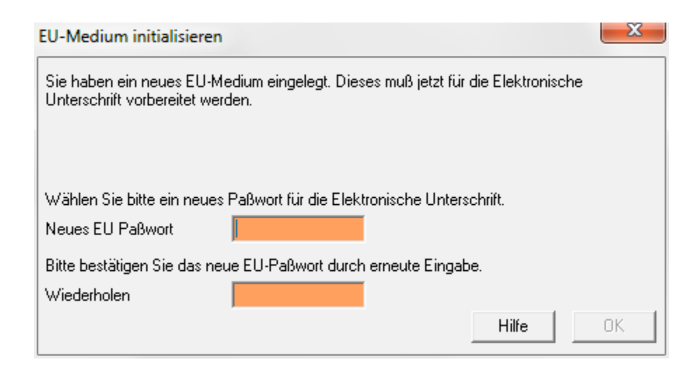
Zur Durchführung der Elektronischen Unterschrift ist ein Schlüsselmedium erforderlich, auf der sich der mit dem EU-Passwort verschlüsselte "Private Key" befindet.
Der dazugehörige "Public Key" ist auf Ihrer Festplatte in der Datei "<Benutzer>.<EU-Version>.PUB" abgelegt. Dieser Schlüssel muss unter Nutzung der Auftragsart PUB an Ihre Bank übertragen werden.
Bereits auf einem Schlüsselmedium befindliche Schlüssel können in das System übernommen werden.

Ein Assistent geleitet Sie durch die notwendigen Schritte, die nötig sind, um ein (neues) Schlüsselpaar zu erzeugen / zu versenden bzw. ein bereits erzeugtes in das System zu übernehmen:

1 **EU-Medium initialisieren**
Im ersten Schritt werden Sie aufgefordert, das gewählte EU-Medium (s. Kapitel 6.1.5: *Registerkarte Elektronische Unterschrift*) einzulegen. Bestätigen Sie nach dem Einlegen das entsprechende Hinweisfenster mit [***OK***].



Handelt es sich um ein neues (d. h. leeres) EU-Medium, schließt sich hieran die Vergabe eines **EU-Passwort**es (EU-PIN) für den Zugang zum EU-Medium an.
Die Eingabe des Passwortes erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt. Aus Sicherheitsgründen müssen Sie die Eingabe des EU-Passwortes **wiederholen**.



☞ **Beachten Sie bitte:**
Sie müssen das EU-Passwort immer dann eingeben, wenn Sie einen Auftrag unterschreiben wollen. Ohne gültiges EU-Passwort können Sie keine Elektronische Unterschrift leisten.
Eine Änderung des EU-Passwortes nehmen Sie über den Menüpunkt -Kommunikation- / -EU-Passwort ändern- vor.

2 **Erzeugen eines neuen EU-Schlüsselpaares / Übernahme von Schlüsseln**

Für **jeden** zur Durchführung einer Elektronischen Unterschrift berechtigten **Benutzer** muss ein gesondertes Schlüsselpaar erstellt werden.



Im Dialogfenster ist das Feld "**Neues Schlüsselpaar erzeugen**" bereits markiert.
Zur Erzeugung eines neuen Schlüsselpaares geben Sie dann eine beliebige Zeichenkette bestehend aus exakt **32 Zeichen** ein.
Die Zeichenkette kann eine willkürliche Kombination aus Buchstaben, Zahlen und Sonderzeichen sein. Die Eingabe erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt. Diese frei wählbare Zeichenkette bildet die Basis zur Erstellung des Schlüsselpaares.



Sollen vorhandene (z. B. früher erzeugte) Schlüssel an die Bank(en) versandt werden bzw. sollen bereits auf einem Schlüsselmedium befindliche Schlüssel in das System übernommen werden, demarkieren Sie das oben genannte Kontrollkästchen.
Beim Import bereits vorhandener Schlüssel müssen Sie zusätzlich in einem Feld darunter <u>einmal</u> das aktuell gültige **EU-Passwort** eingeben.
Die Eingabe des Passwortes erfolgt verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt.

Anschließend bestätigen Sie Ihre Eingaben über die Schaltfläche [***Weiter >***].

Übrigens:

Die **Schlüsselberechnung** beruht auf Primzahlen, die aufgrund der eingegebenen Zeichenkette gebildet werden. Die Suche nach gültigen Primzahlen kann einige Zeit in Anspruch nehmen.

Gleichzeitig mit dem Speichern des "Private Key" auf dem EU-Medium wird der "Public Key" in eine Datei kopiert, damit er an Ihre Bank übertragen werden kann. Ihre Bank benötigt den "Public Key" zur Prüfung Ihrer elektronischen Unterschrift.

Der "Public Key" wird im Unterverzeichnis ..\DAT in einer Datei mit der Extension "**.PUB**" abgelegt. Der eigentliche Dateiname wird aus dem Benutzernamen des angemeldeten Benutzers und der EU-Version gebildet.

Beispiel:
Heißt der angemeldete Benutzer "meier" und erstellt Herr Meier ein Schlüsselpaar, so wird im Unterverzeichnis ..\DAT eine Datei MEIER.<EU-Version>.PUB angelegt. Diese Datei enthält dann den an die Bank zu übertragenden "Public Key".

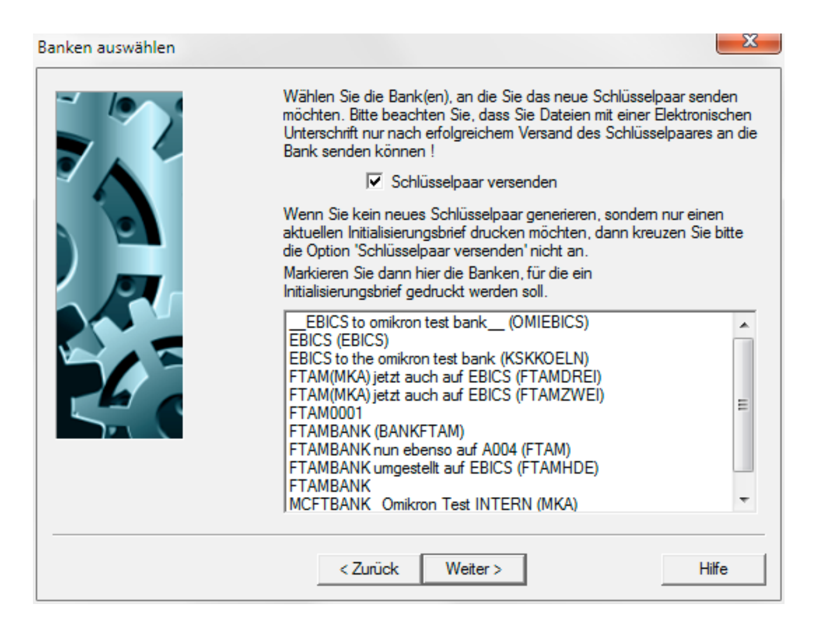
Der von der Bank zur Prüfung Ihrer Elektronischen Unterschrift benötigte Public Key muss unter Nutzung der Auftragsart **PUB** an die Bank verschickt werden.



Wenn Sie vor Durchführung Ihres Initialisierungsauftrages (Auftragsart **INI**) das Keypaar generieren, so wird der öffentliche Schlüssel automatisch im Rahmen der Initialisierung an die Bank übertragen.

Beachten Sie bitte:
Nach jeder Neuerstellung eines Schlüsselpaares **müssen** Sie zur Durchführung einer Elektronischen Unterschrift den neuen Public Key an die Bank übertragen.

3 **Auswahl der Bank(en)**
Wählen Sie mittels Mausklick die Bank(en), an die Sie das neue Schlüsselpaar senden möchten, aus der Liste unterhalb des bereits markierten Feldes "**Schlüsselpaar versenden**" aus.



Wenn Sie lediglich einen aktuellen Initialisierungsbrief drucken und kein neues Schlüsselpaar versenden möchten, entfernen Sie bitte die Markierung im Kontrollkästchen.
Sie können in einer Liste der verfügbaren Banken eine oder mehrere Banken markieren, für die ein Initialisierungsbrief gedruckt werden soll.
Drücken Sie anschließend auf die Schaltfläche [***Weiter >***].

Beachten Sie bitte:
Dateien mit einer Elektronischen Unterschrift können Sie erst **nach** dem erfolgreichen Versand des Schlüsselpaares an die Bank senden.

4 **DFÜ-Passwort eingeben**
Unterhalb der ausgewählten Bank müssen Sie nun das gültige **DFÜ-Passwort** eingeben.
Es wird zur Legitimation des DFÜ-Auftrags bei der Bank benötigt.
Haben Sie mehrere Banken ausgewählt, können Sie durch Markieren des Kontrollkästchens "**Dasselbe DFÜ-Passwort bei allen Banken benutzen**" bestimmen, dass bei allen Banken dasselbe DFÜ-Passwort verwendet wird. Andernfalls lassen Sie diese Option unmarkiert. Es wird dann anschließend für jede gewählte Bank das aktuell gültige DFÜ-Passwort abgefragt.
Die Passwortvergabe erfolgt verdeckt, d. h. jeder Tastendruck wird durch ein * (Sternchen) dargestellt.

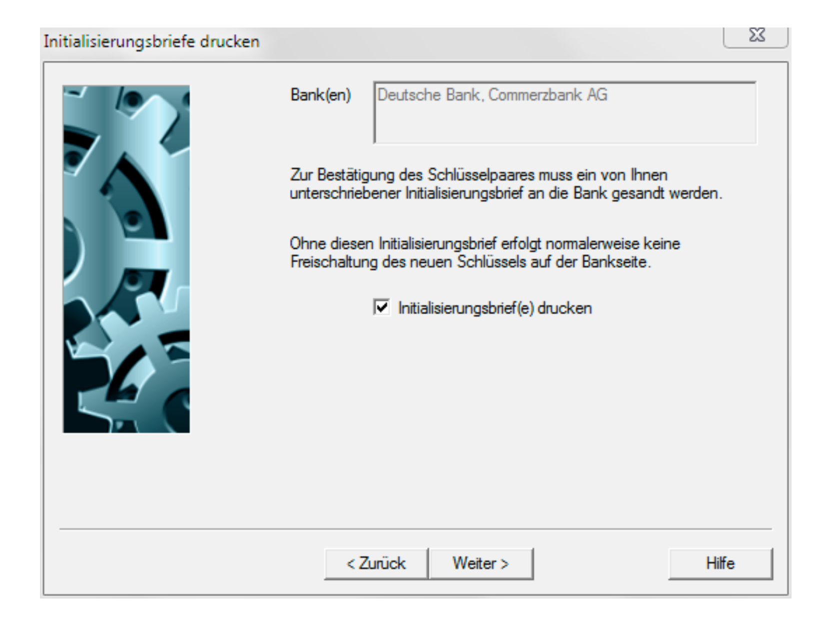




Sie schließen die DFÜ-Passworteingabe ab, indem Sie wiederum die Schaltfläche [***Weiter >***] drücken.

5 **Initialisierungsbrief(e) drucken**

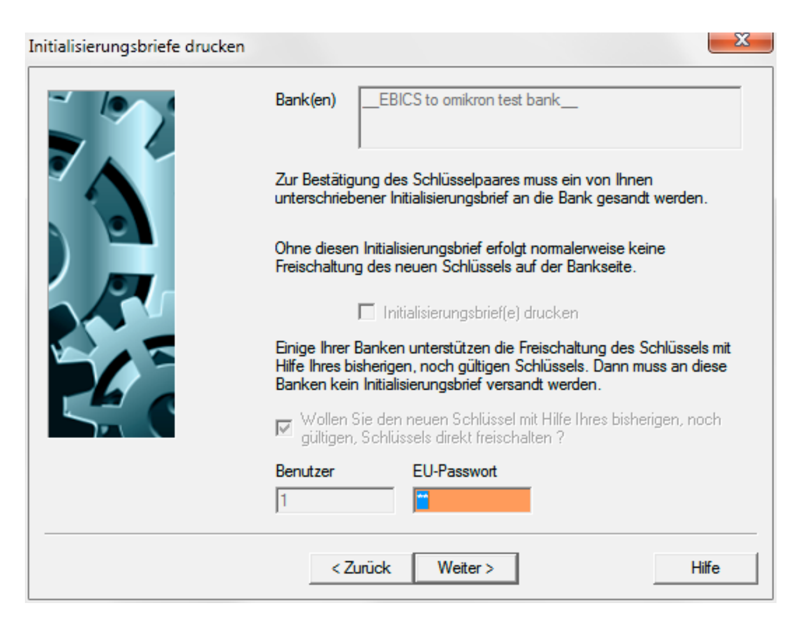
Zur Bestätigung des (neuen) Schlüsselpaares muss ein von Ihnen unterschriebener Initialisierungsbrief an die Bank (oder an mehrere) gesandt werden. Ohne diesen Initialisierungsbrief erfolgt normalerweise keine Freischaltung des neuen Schlüssels auf der Bankseite.
Die Option "**Initialisierungsbrief(e) drucken**" ist bereits markiert.



Möchten Sie keine(n) Initialisierungsbrief(e) drucken, entfernen Sie bitte die entsprechende Markierung.
Einige Banken erlauben die Freischaltung des Schlüssels mit Hilfe Ihres bisherigen, noch gültigen Schlüssels. Dann muss kein Initialisierungsbrief an die Bank gesandt werden (s. dazu: *Versand von PUB-Aufträgen mit EU* in Kapitel 6.3).
Wenn von der Bank so vorgesehen, können Sie in einem weiteren Feld Ihr gültiges **EU-Passwort** eingeben, um den neuen Schlüssel mit Hilfe Ihres noch gültigen bisherigen Schlüssels direkt freizuschalten.



Bei EBICS kann ein Teilnehmer im Zustand "Bereit" seine bankfachlichen Schlüssel mittels PUB-Auftrag aktualisieren. Nach Auswahl einer EBICS-BPD ist das Kontrollkästchen zur Schlüsselaktivierung markiert und gesperrt.
Sie müssen Ihr Signaturmedium einlegen und das Signaturpasswort (**EU-Passwort**) eingeben. Der neue Schlüssel wird dann mit dem alten unterschrieben. Ein Initialisierungsbrief wird dann für den EBICS-Zugang nicht erstellt, da die Authentizität der übermittelten Schlüssel durch die EU gesichert wird.

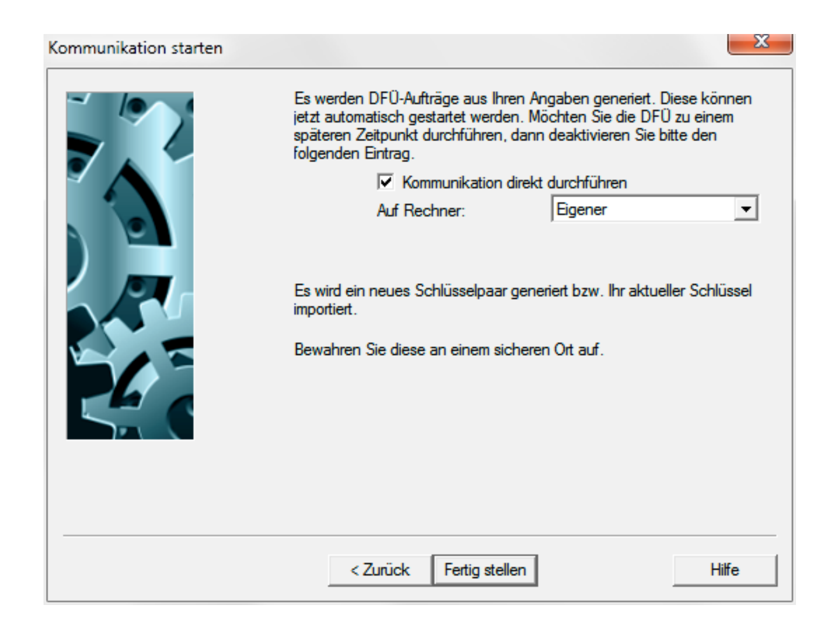


Eine Ausnahme besteht, wenn Sie eine Chipkarte verwenden, die nur den jeweils aktuellen Schlüssel enthält. In diesem Fall müssen Sie zuerst Ihren Bankzugang sperren (SPR-Auftrag). Im Anschluss daran führen Sie dann eine Initialisierung mit Ihrer neuen Chipkarte durch. Anschließend drücken Sie auf die Schaltfläche [***Weiter >***].

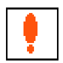
Über die Schaltfläche [**< *Zurück***] können Sie jeweils die Arbeitsschritte zurückgehen, um ggf. Änderungen einzugeben.

6 **Kommunikation starten**
Es wird eine DFÜ-Auftragsdatei aus Ihren Angaben generiert. Die DFÜ kann in diesem letzten Schritt automatisch gestartet werden, wenn Sie den voreingestellten Eintrag über die Schaltfläche [***Fertig stellen***] bestätigen. Möchten Sie die DFÜ zu einem späteren Zeitpunkt durchführen, deaktivieren Sie bitte den Eintrag "**Kommunikation direkt durchführen**".
Falls Sie in einer Netzwerkumgebung arbeiten, können Sie einen möglicherweise speziell für Kommunikationsaufträge vorgesehenen Rechner über das Listenfeld "**Auf Rechner:**" auswählen und die Kommunikation dort starten.





Es wird zunächst das neue Schlüsselpaar für die Elektronische Unterschrift generiert. bzw. Ihr aktueller Schlüssel in das System übernommen.



Bewahren Sie das EU-Medium **immer** an einem sicheren Ort auf!

Nutzen Sie die Möglichkeit zur direkten Freischaltung des Schlüssels (durch *Versand von PUB-Aufträgen mit EU*), schließt sich hieran direkt die Leistung der Elektronischen Unterschrift an.

Abschließende Hinweise nach erfolgreicher Erstellung des Schlüssels (wie z. B. auf die Erstellung eines DFÜ-Auftrages zum späteren Versenden des Schlüssels) quittieren Sie durch Drücken von [***OK***].

Anschließend werden Initialisierungsbriefe für jede ausgewählte Bank gedruckt. Bitte senden Sie diese unterschrieben zur Freischaltung des Schlüsselpaares an die Bank.



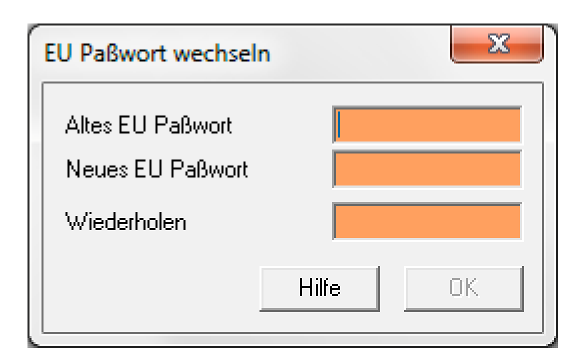
6.2 EU-Passwort ändern

Das EU-Passwort dient der Verschlüsselung des auf dem EU-Medium abgespeicherten Private Keys. Sie können eine Elektronische Unterschrift nur nach Eingabe Ihres EU-Passwortes leisten.

Sollte sich die Notwendigkeit einer Änderung des EU-Passwortes ergeben, so wählen Sie aus dem Menü -Kommunikation- den Menüpunkt -EU-Passwort ändern- aus.

Zunächst werden Sie aufgefordert, das **EU-Medium** einzulegen, damit der auf dem Medium enthaltene Private Key im Anschluss mit dem neuen EU-Passwort verschlüsselt werden kann. Drücken Sie nach dem Einlegen des Mediums die Schaltfläche [***OK***].

Das Programm fordert Sie dann auf, das bisher verwendete **(alte) EU-Passwort** einzugeben. Im Anschluss geben Sie dann das **neue EU-Passwort** ein. Die Eingaben erfolgen verdeckt, d. h. jedes eingegebene Zeichen wird durch ein * (Sternchen) dargestellt. Aus Sicherheitsgründen müssen Sie die Eingabe des neuen EU-Passwortes **wiederholen**. Sie bestätigen Ihre Eingaben durch Anwahl der Schaltfläche [***OK***].



Die abschließende Meldung bestätigen Sie ebenfalls mit [***OK***].



Da es sich in diesem Fall nur um eine neue Verschlüsselung und nicht um eine Änderung des Private Keys handelt, erübrigt sich eine Übertragung des Public Keys an Ihre Bank.



6.3 Unterschriftsversion umstellen

Nachfolgend sind zwei Umstellungsassistenten beschrieben, die den Umstieg auf neue Versionen der Elektronischen Unterschrift erleichtern:

Kapitel 6.3.1: *Umstellung der EU-Version von A003 auf A004*

Beachten Sie bitte: Diese Umstellung ist nur für FTAM-/FTP-Zugänge möglich.

Kapitel 6.3.2: *Umstellung der EU-Version von A004 auf A005 / A006*

Beachten Sie bitte: Diese Umstellung ist nur für EBICS-Zugänge möglich.

Da EBICS die EU-Version A003 nicht unterstützt, ist die direkte Umstellung von A003 auf A005/A006 **nicht** möglich!

Zur grundsätzlichen Umstellung des DFÜ-Verfahrens von FTAM/FTP auf EBICS siehe:

Kapitel 4.6: *FTAM-/FTP-Bankzugang auf EBICS umstellen*

Beachten Sie bitte: Diese Umstellung ist nur für FTAM-/FTP-Zugänge mit A004-EU möglich.



6.3.1 Umstellung der EU-Version von A003 auf A004 (nur für FTAM-/FTP-Zugänge)

Ab der Programmversion 3.01.001 wird die Elektronische Unterschrift in den neuen Versionen A004/M002 unterstützt, die mit Signierschlüsseln von 1024 Bit Länge arbeiten:

FTAM/FTP: Unterschrifts-Version A004

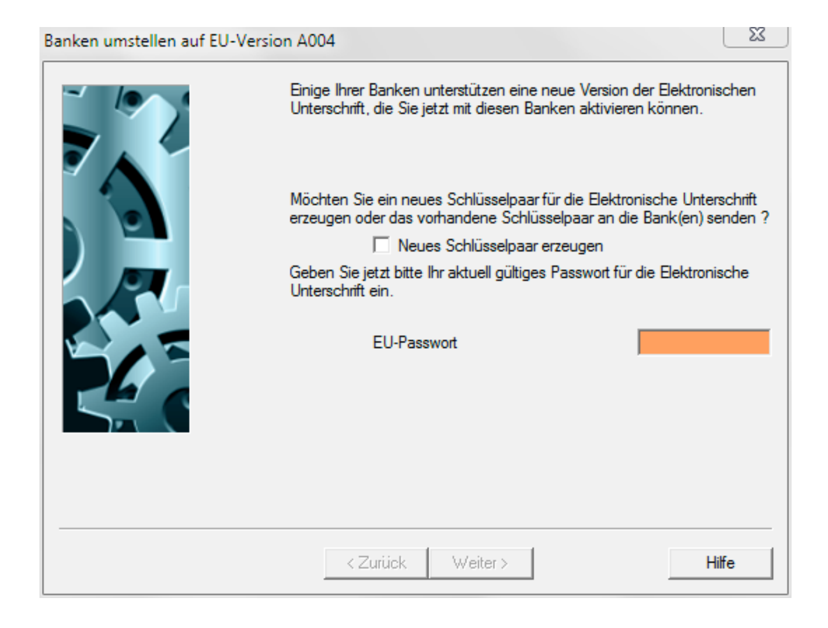
MCFT: Unterschrifts-Version M002

Zusätzlich zur Verlängerung der Signierschlüssel wurde mit den Banken vereinbart, den Versand eines neuen Public Key mit Elektronischer Unterschrift zu unterstützen, damit der Übergang auf die neue Unterschrift erleichtert wird.

Während die Schlüssel bei MCFT im Rahmen der Kommunikation mit der Bank vollautomatisch umgestellt werden, ermöglicht bei FTAM-/FTP-Zugängen eine komfortable Umstellungsfunktion den reibungslosen Übergang zu den neuen Versionen.

Sobald Sie von einer Bank eine Bankparameterdatei abgeholt haben/erhalten haben, in der Ihrem System anhand des Bankparameterstrings die Unterstützung der neuen Unterschriftsversion signalisiert wird, werden Sie beim Start des Programms durch ein Fenster auf den Sachverhalt der nun möglichen Umstellung hingewiesen ("**Banken umstellen auf EU-Version A004**").

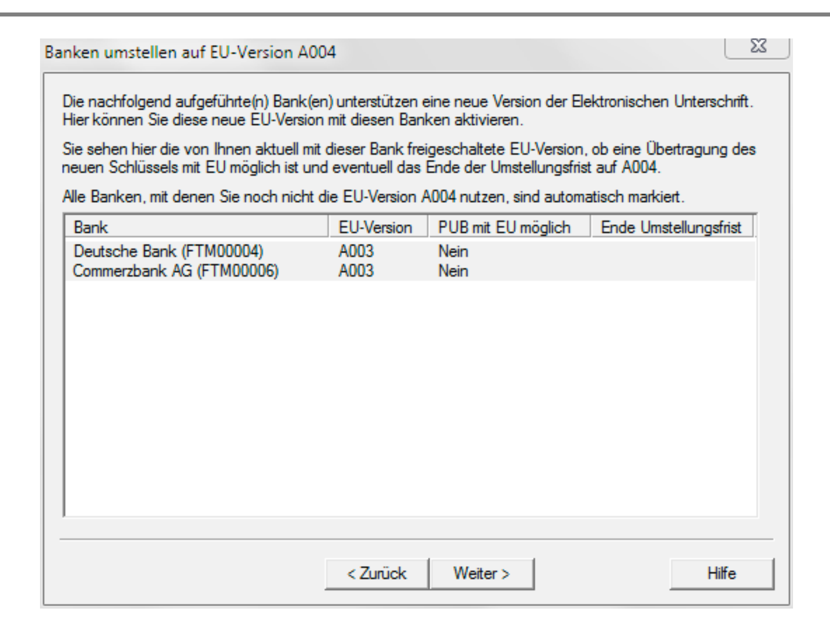
Um ein neues Schlüsselpaar für die neue EU-Version zu erzeugen oder ein bereits erzeugtes Schlüsselpaar an die Bank(en) zu senden, folgen Sie den in Kapitel 6.1 beschriebenen Handlungsanweisungen ("Neues Schlüsselpaar erzeugen").
Generieren Sie ein neues Schlüsselpaar, so erfolgt dies sowohl im Format A003 als auch im Format A004. Beim späteren Ausführen des PUB-Auftrages wird dann an die Banken, die die Unterstützung der neuen EU-Version signalisiert haben, der Public Key im neuen Format versandt.
Über die Schaltfläche [***Weiter>***] gelangen sie jeweils zum nächsten Schritt des Assistenten.



Neben dem(n) Namen der Bank(en), die die Umstellmöglichkeit anbietet(n), finden sie jeweils Informationen über die aktuell mit dieser Bank freigeschaltete EU-Version (A003), ob eine Übertragung des neuen Schlüssels mit Elektronischer Unterschrift möglich ist und gegebenenfalls auch das Ende der Umstellungsfrist auf die neue EU-Version A004. Alle Banken, mit denen Sie noch nicht die neue EU-Version A004 nutzen, sind automatisch markiert.

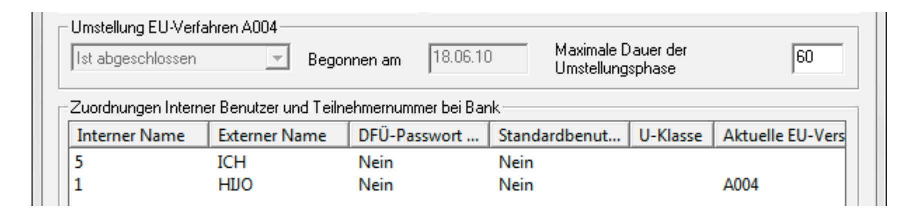
6.3.1 Umstellung der EU-Version von A003 auf A004 (nur für FTAM-/FTP-Zugänge)





Sollte die Bank den Versand von PUB-Aufträgen mit Elektronischer Unterschrift unterstützen, können Sie den neuen Schlüssel direkt mit Hilfe Ihres bisherigen, noch gültigen Schlüssels, freischalten. Dann entfällt der Versand eines Initialisierungsbriefes an die Bank. Geben Sie dazu beim Durchlaufen des Assistenten an der Stelle, wo der Druck der Initialisierungsbriefe initiiert wird, Ihr gültiges EU-Passwort in das entsprechende Feld ein und schließen Sie den Assistenten ab. Bei positiver EU-Prüfung mit Ihrem alten Schlüssel wird der neue Schlüssel automatisch aktiviert und freigeschaltet.
Bei fehlgeschlagener Unterschriftsprüfung wird der Schlüsselstatus bei der Bank auf "Initialisiert "gesetzt und kann wie bisher manuell per Initialisierungsbrief freigeschaltet werden. Das gleiche gilt beim Versand von PUB-Aufträgen ohne EU.

Nach der Umstellung leisten Sie Unterschriften im Format A004, die mit Unterschriften im Format A003 von anderen Teilnehmern kombiniert sein können, bis alle Teilnehmer ihre Unterschriftsversionen umgestellt haben.
Die jeweils aktuell verwendete EU-Version wird in den FTAM- bzw. FTP-Bankparameterdateien für jeden Teilnehmer angezeigt zusammen mit Informationen zum Status der Umstellung des EU-Verfahrens (kann beginnen, hat begonnen, ist abgeschlossen), zum Beginn der Umstellung und zur maximalen Dauer der Umstellungsphase (standardmäßig 60 Tage).





6.3.2 Umstellung der EU-Version auf A005 / A006 bzw. M005 / M006

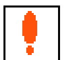
Ab der Programmversion 3.22.001 wird die Elektronische Unterschrift in den neuen Versionen A005 / A006 bzw. M005 / M006 unterstützt, die mit Signaturschlüsseln von 1536-4096 Bit Länge arbeiten (Standard: 2048).

EBICS: Unterschrifts-Version A005 / A006 (EBICS-Version 2.4, EBICS-Protokollversion H003)

A005 bei Chipkarten, die nur diese unterstützen
A006 immer bei Software-EU/EU-Server / bei übrigen Chipkarten

MCFT: Unterschrifts-Version M005 / M006 analog

Gleichermaßen für EBICS wie für MCFT wird jedem Benutzer beim ersten Programmstart des Tages mit einem Assistenten die Umstellung seiner Signaturschlüssel angeboten, wenn die Banksysteme die Unterstützung der neuen Verfahren signalisiert haben (s. z. B. Kapitel 3.5: *EBICS*: EBICS-Parameter). Sie können diesen Assistenten einfach abbrechen, wenn Sie die Umstellung z. Z. nicht durchführen möchten.



Die Schlüssel-Dateien werden jetzt konvertiert und können danach in älteren Programmversionen nicht mehr verwendet werden!

Wenn Sie sich für die Umstellung der Signaturen entscheiden, werden Sie folgendermaßen durch den Umstellungsprozess geführt:

1.

Wenn Sie mit einer Chipkarte arbeiten, beachten Sie bitte folgenden Sonderfall: Manche Chipkarten unterstützen das Generieren von neuen Schlüsseln nicht (z. B. die SECCOS-Karte der deutschen Kreditwirtschaft). Wenn Sie mit einer solchen Karte arbeiten, können Sie erst dann umstellen, wenn Sie eine neue Karte erhalten haben. Da der neue Schlüssel mit dem alten unterschrieben wird, muss während der Umstellungsprozedur die Chipkarte gewechselt werden. In diesem Fall verhält sich das System folgendermaßen:

Wenn sich beim ersten Programmstart des Tages keine Chipkarte im Leser befindet und alle vorhandenen Banken signalisiert haben, dass sie die neuen Signaturversionen A005/A006 oder M005/M006 unterstützten, wird folgender Hinweis angezeigt:

Wenn Sie eine neue Signaturkarte erhalten haben und jetzt Ihre Signatur auf die neue empfohlene Version umstellen möchten, legen Sie jetzt diese neue Karte ein und führen den Assistenten bis zum Ende durch!

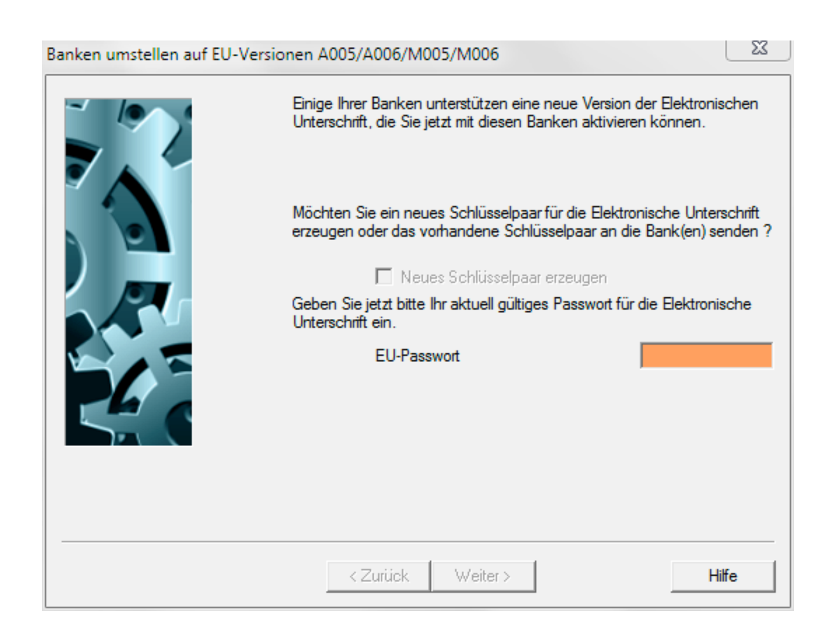
Legen Sie nun die neue Chipkarte ein und fahren Sie fort.

2.

Bei Verwendung der SECCOS-Chipkarte werden nun die vorhandenen Schlüssel von der neuen Karte importiert.

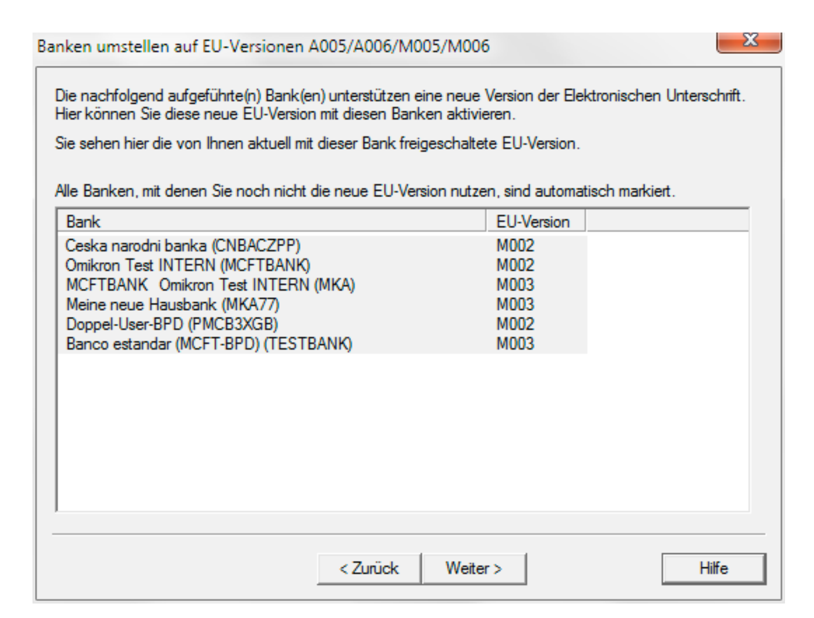
Bei allen anderen Signaturmedien erzeugen Sie ein neues Schlüsselpaar für die neuen Signaturverfahren. Die bisher verwendeten Schlüssel bleiben dabei unverändert erhalten, so dass Sie die neuen Schlüssel mit den alten unterschreiben können:





3.

Im nächsten Schritt werden alle Banken angezeigt, für die die Signatur umgestellt werden kann. Sie sollten alle Banken zusammen umstellen:



4.

Anschließend wird das Kommunikationspasswort abgefragt.

5.

Durch Eingabe Ihres EU-Passwortes signieren Sie nun den neuen öffentlichen Schlüssel (mit Ihrem alten), so dass kein Bestätigungsbrief und keine Freischaltung durch die Bank erforderlich ist.

Bitte beachten Sie, dass für EBICS ein Schlüsselwechsel ohne Signatur nicht vorgesehen ist.




Bei Verwendung der SECCOS-Chipkarte werden Sie nun aufgefordert, die alte Karte einzulegen, da die Signatur des neuen Schlüssels mit der alten Karte erfolgen muss:

Bitte entnehmen Sie die neue Chipkarte und legen Sie jetzt Ihre bisherige, noch gültige, Chipkarte ein

6.

Wenn Sie die folgende Anzeige sehen, ist der Schlüsselwechsel abgeschlossen und Sie können sofort mit den neuen Schlüsseln weiter arbeiten:

Alle Übertragungen wurden erfolgreich durchgeführt!



Beispiel für Initialisierungsbrief EU

```
Benutzername                    Meier
Datum                           23.12.08
Uhrzeit                         13:21
User-ID                         00000001
Bankname                        MCB30
EU-Version                      M002


Öffentlicher Schlüssel (Public Key) für die
Elektronische Unterschrift:

Exponent                      1024

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01


Modulo                        1024

9b 5a 7c f7 9d 49 68 23 38 c7 74 c4 32 df 0d 13
a1 5e 0c 64 9b 24 2c df b8 da 95 5e 53 76 c5 5e
80 00 53 10 b1 cc 3a 72 98 0d 0d 19 23 dd 63 85
ce 35 81 a3 96 44 da c7 5d 62 03 74 57 b3 b4 23
2f 50 24 4c a7 e4 60 4f 0f dc 2e 34 39 11 57 15
6f c0 92 de d1 5d 66 83 93 3c f0 a7 b6 56 35 f0
76 9f a7 b9 9d e0 12 5f 85 91 5e 3c f2 ec e2 60
50 87 b8 f7 36 c6 cf 54 da 7d 8a 8a 82 9d cb 33

Hash           21 33 E7 30
               72 C4 EC EA
               64 DE CC 2B
               2E A7 CD B5
               E1 68 50 AC


Ich bestätige hiermit den obigen öffentlichen
Schlüssel für meine elektronische Unterschrift.


Ort / Datum                     _________________

Firma / Name                    _________________

Unterschrift                    _________________
```



Stichwortverzeichnis


MCC





